

vCloud Director Administrator's Guide

vCloud Director 1.5

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-000636-00

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

Copyright © 2010, 2011 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>.

VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.

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

Contents

vCloud Director Administrator's Guide	7
1 Getting Started with vCloud Director	9
Overview of vCloud Director Administration	9
Log In to the Web Console	11
Preparing the System	12
Create a Microsoft Sysprep Deployment Package	12
Replace a Microsoft Sysprep Deployment Package	13
Set User Preferences	14
Change a System Administrator Password	14
2 Adding Resources to vCloud Director	15
Adding vSphere Resources	15
Adding Cloud Resources	17
3 Creating and Provisioning Organizations	23
Understanding Leases	23
Create an Organization	24
Allocate Resources to an Organization	28
Adding Networks to an Organization	32
4 Creating a Published Catalog	35
Enable Catalog Publishing	35
Create a Published Catalog	36
Upload a vApp Template	36
Import a vApp Template from vSphere	37
Upload a Media File	37
Import a Media File from vSphere	38
Publish a Catalog	38
5 Managing Cloud Resources	39
Managing Provider vDCs	39
Managing Organization vDCs	43
Managing External Networks	49
Managing Organization Networks	50
Managing Network Pools	66
Managing Cloud Cells	67
6 Managing vSphere Resources	69
Managing vSphere vCenter Servers	69
Managing vSphere ESX/ESXi Hosts	71

- Managing vSphere Datastores 72
- Managing Stranded Items 73

7 Managing Organizations 75

- Enable or Disable an Organization 75
- Delete an Organization 75
- Modify an Organization Name 76
- Modify an Organization Full Name and Description 76
- Modify Organization LDAP Options 76
- Modify Organization Catalog Publishing Policy 77
- Modify Organization Email Preferences 78
- Modify Organization Lease, Quota, and Limit Settings 78
- Add a Catalog to an Organization 79
- Managing Organization Resources 79
- Managing Organization Users and Groups 80
- Managing Organization vApps and Virtual Machines 80

8 Managing System Administrators and Roles 83

- Add a System Administrator 83
- Import a System Administrator 84
- Enable or Disable a System Administrator 84
- Delete a System Administrator 84
- Edit System Administrator Profile and Contact Information 84
- Send an Email Notification to Users 85
- Delete a System Administrator Who Lost Access to the System 85
- Import an LDAP Group 85
- Delete an LDAP Group 86
- Change an LDAP Group Description 86
- Roles and Rights 86
- Create a Role 86
- Copy a Role 87
- Edit a Role 87
- Delete a Role 87

9 Managing System Settings 89

- Modify General System Settings 89
- General System Settings 90
- Configure SMTP Settings 91
- Configure System Notification Settings 91
- Configuring Blocking Tasks and Notifications 92
- Configuring the System LDAP Settings 93
- Customize the vCloud Director Client UI 96
- Configure the Public Web URL 97
- Configure the Public Console Proxy Address 98
- Configure the Public REST API Base URL 98
- Configure the Account Lockout Policy 98

10	Monitoring vCloud Director	101
	Viewing Tasks and Events	101
	Monitor and Manage Blocking Tasks	103
	View Usage Information for a Provider vDC	103
	View Usage Information for an Organization vDC	103
	Using vCloud Director's JMX Service	104
	Viewing the vCloud Director Logs	104
	vCloud Director and Cost Reporting	104
	Monitoring Quarantined Files	105
11	Roles and Rights	107
	Predefined Roles and Their Rights	107
	Index	111

vCloud Director Administrator's Guide

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

Intended Audience

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

Getting Started with vCloud Director

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

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

This chapter includes the following topics:

- [“Overview of vCloud Director Administration,”](#) on page 9
- [“Log In to the Web Console,”](#) on page 11
- [“Preparing the System,”](#) on page 12
- [“Create a Microsoft Sysprep Deployment Package,”](#) on page 12
- [“Replace a Microsoft Sysprep Deployment Package,”](#) on page 13
- [“Set User Preferences,”](#) on page 14
- [“Change a System Administrator Password,”](#) on page 14

Overview of vCloud Director Administration

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

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

vSphere Resources

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

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

Cloud Resources

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

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

Provider Virtual Datacenters

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

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

Organization Virtual Datacenters

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

A single organization can have multiple organization vDCs.

vCloud Director Networking

vCloud Director supports three types of networks.

- External networks
- Organization 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 vCloud 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 vCloud Director User's Guide*.

Network Pools

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

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

Only system administrators can create and manage network pools.

Organizations

vCloud Director supports multi-tenancy through the use of organizations. An organization is a unit of administration for a collection of users, groups, and computing resources. Users authenticate at the organization level, supplying credentials established by an organization administrator when the user was created or imported. System administrators create and provision organizations, while organization administrators manage organization users, groups, and catalogs. Organization administrator tasks are described in the *VMware vCloud Director User's Guide*.

Users and Groups

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

Catalogs

Organizations use catalogs to store vApp templates and media files. The members of an organization that have access to a catalog can use the catalog's vApp templates and media files to create their own vApps. A system administrator can allow an organization to publish a catalog to make it available to other organizations. Organizations administrators can then choose which catalog items to provide to their users.

Log In to the Web Console

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

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

Prerequisites

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

Procedure

- 1 Open a Web browser and navigate to **https://hostname.domain.tld/cloud**.

For *hostname.domain.tld*, provide the fully qualified domain name associated with the primary IP address of the vCloud Director server host. For example, **https://cloud.example.com/cloud**.

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

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

Preparing the System

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

For more information about each task, see [Table 1-1](#).

Table 1-1. Quick Start Tasks

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 43
Add a Network to an Organization	"Creating Organization Networks," on page 50
Add a Catalog to an Organization	"Add a Catalog to an Organization," on page 79

Create a Microsoft Sysprep Deployment Package

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

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

Prerequisites

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 vCloud Director server host.

Each operating system requires its own folder.

NOTE Folder names are case-sensitive.

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

`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 vCloud Director server host.

Each operating system requires its own folder.

NOTE Folder names are case-sensitive.

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

`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**.

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 vCloud Director

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

This chapter includes the following topics:

- [“Adding vSphere Resources,”](#) on page 15
- [“Adding Cloud Resources,”](#) on page 17

Adding vSphere Resources

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

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

Attach a vCenter Server

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

Prerequisites

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

Procedure

- 1 [Open the Attach New vCenter Wizard](#) on page 16
Open the Attach New vCenter wizard to start the process of attaching a vCenter Server to vCloud Director.
- 2 [Provide vCenter Server Connection and Display Information](#) on page 16
To attach a vCenter Server to vCloud Director, you must provide connection information and a display name for the vCenter Server.
- 3 [Connect to vShield Manager](#) on page 16
vCloud Director requires vShield Manager to provide network services. Each vCenter Server you attach to vCloud Director requires its own vShield Manager.
- 4 [Confirm Settings and Attach the vCenter Server](#) on page 16
Before you attach the new vCenter Server, review the settings you entered.

Open the Attach New vCenter Wizard

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

Procedure

- 1 Click the **Manage & Monitor** tab and then click **vCenters** in the left pane.
- 2 Click the **Attach New vCenter** button.

The Attach New vCenter wizard launches.

Provide vCenter Server Connection and Display Information

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

Procedure

- 1 Type the host name or IP address of the vCenter Server.
- 2 Select the port number that vCenter Server uses.
The default port number is 443.
- 3 Type the user name and password of a vCenter Server administrator.
The user account must have the Administrator role in vCenter.
- 4 Type a name for the vCenter Server.
The name you type becomes the display name for the vCenter Server in vCloud Director.
- 5 (Optional) Type a description for the vCenter Server.
- 6 Click **Next** to save your choices and go to the next page.

Connect to vShield Manager

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

Procedure

- 1 Type the host name or IP address of the vShield Manager to use with the vCenter Server that you are attaching.
- 2 Type the user name and password to connect to vShield Manager.
The default user name is **admin** and the default password is **default**. You can change these defaults in the vShield Manager user interface.
- 3 Click **Next** to save your choices and go to the next page.

Confirm Settings and Attach the vCenter Server

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

Procedure

- 1 Review the settings for the vCenter Server and vShield Manager.
- 2 (Optional) Click **Back** to modify the settings.
- 3 Click **Finish** to accept the settings and attach the vCenter Server.

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

What to do next

Assign a vShield for VMware vCloud Director license key in the vCenter Server.

Assign a vShield License Key in vCenter

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

Prerequisites

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

Procedure

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

Use the vShield for VMware vCloud Director license key you received when you purchased vCloud Director. You can use this license key in multiple vCenter Servers.

- 6 Click **OK**.

Adding Cloud Resources

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

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

For more information about organization virtual datacenters, see [“Allocate Resources to an Organization,”](#) on page 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

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

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

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

Prerequisites

Verify that at least one vCenter Server is attached with an available resource pool to vCloud Director. The resource pool must be in a vCenter cluster that is configured to use automated DRS. The vCenter Server must have the vShield for VMware vCloud Director license key.

Procedure

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

- 2 Click **New Provider vDC**.

- 3 Type a name and optional description.

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

- 4 Select the latest supported hardware version and click **Next**.

This selection determines the latest supported hardware version for virtual machines in organization vDCs based on this provider vDC. **Hardware Version 8** requires ESX/ESXi 5.0 hosts. If this provider vDC will use a resource pool that contains ESX/Esxi 5.0 and ESX/ESXi 4.x hosts, select **Hardware Version 7**.

- 5 Select a vCenter Server and resource pool and click **Next**.

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

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

vCloud 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 might appear. Do not add these datastores to your provider vDC.

Use only shared storage because vSphere DRS cannot migrate virtual machines on local storage.

- 7 Type the root user name and password for the ESX/ESXi hosts and click **Next**.

- 8 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 vCloud Director to use. You can create organization networks that connect to an external network.

Prerequisites

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

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

Add a Network Pool That Is Backed by VLAN IDs

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

Prerequisites

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



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

Procedure

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

What to do next

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

Add a Network Pool That Is Backed by Cloud Isolated Networks

You can create a network pool that is backed by cloud isolated networks. A cloud isolated network spans hosts, provides traffic isolation from other networks, and is the best source for vApp networks.

An isolation-backed network pool does not require preexisting port groups in vSphere.

Prerequisites

Verify that a vSphere distributed switch is available.

Procedure

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

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

What to do next

You can now create an organization 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

You can add a network pool that is backed by port groups to register vSphere port groups for vCloud Director to use. Unlike other types of network pools, a network pool that is backed by port groups does not require a vSphere distributed switch.



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

Prerequisites

Verify that one or more port groups are available in vSphere. The port groups must be available on each ESX/ESXi host in the cluster, and each port group must use only a single VLAN. Port groups with VLAN trunking are not supported.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.
- 2 Click **Add Network Pool**.
- 3 Select **vSphere Port Group-backed** and click **Next**.
- 4 Select a vCenter Server and click **Next**.

- 5 Select one or more port groups, click **Add**, and click **Next**.

You can create one network for each port group.

- 6 Type a name and optional description for the network and click **Next**.
- 7 Review the network pool settings and click **Finish**.

What to do next

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

Set the MTU for a Network Pool Backed by Cloud Isolated Networks

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

When you configure the virtual machine guest operating system and the underlying physical infrastructure with the standard MTU (1500 bytes), the VMware network isolation protocol fragments frames. To avoid frame fragmentation, increase the MTU to at least 1524 bytes for the network pool and the underlying physical network. You can increase the network pool MTU up to, but not greater than, the MTU of the physical network.

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

Prerequisites

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.
- 2 Right-click the network pool name and select **Properties**.
- 3 On the **Network Pool MTU** tab, type the MTU and click **OK**.

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

Creating and Provisioning Organizations

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,”](#) on page 23
- [“Create an Organization,”](#) on page 24
- [“Allocate Resources to an Organization,”](#) on page 28
- [“Adding Networks to an Organization,”](#) on page 32

Understanding Leases

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

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

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

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

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

For more information about specifying lease settings, see [“Configure Organization Lease, Quota, and Limit Settings,”](#) on page 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 users 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 26
vCloud Director requires an SMTP server to send user notification and system alert emails. An organization can use the system email settings or use its own email settings.
- 7 [Configure Organization Lease, Quota, and Limit Settings](#) on page 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 27
Before you create the organization, review the settings you entered.

Open the New Organization Wizard

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

Procedure

- 1 Click the **Manage & Monitor** tab and then click **Organizations** in the left pane.
- 2 Click the **New Organization** button.
The New Organization wizard starts.

Name the Organization

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

Procedure

- 1 Type an organization name.

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

- 2 Type a display name for the organization.

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

- 3 (Optional) Type a description of the organization.

- 4 Click **Next**.

Specify the Organization LDAP Options

You can use an LDAP service to provide a directory of users and groups for the organization. If you do not specify an LDAP service, you must create a user account for each user in the organization. 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 93.

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 vCloud 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 users 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 (Optional) Type the contact information for the user.
- 5 Select **Unlimited** or type a user quota for stored and running virtual machines and click **OK**.
These quotas limit the user's ability to consume storage and compute resources in the organization.
- 6 Click **Next**.

Set the Organization Catalog Publishing Policy

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

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

Procedure

- 1 Select a catalog publishing option.

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

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

Procedure

- 1 Select an SMTP server option.

Option	Description
Use 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 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 run and that vApps and vApp templates can be stored. You can also specify what happens to vApps and vApp templates when their storage lease expires.

- 2 Select the quotas for running and stored virtual machines.

Quotas determine how many virtual machines each user in the organization can store and power on in the organization's virtual datacenters. The quotas that you specify act as the default for all new users added to the organization.

- 3 Select the limits for resource intensive operations.

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

- 4 Select the number of simultaneous VMware Remote Console connections for each virtual machine.

You might want to limit the number of simultaneous connections for performance or security reasons.

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

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

Confirm Settings and Create the Organization

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

Procedure

- 1 Review the settings for the organization.
- 2 (Optional) Click **Back** to modify the settings.

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

What to do next

Allocate resources to the organization.

Allocate Resources to an Organization

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

Prerequisites

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

Procedure

- 1 [Open the Allocate Resources Wizard](#) on page 28
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 29
Configure the allocation model to specify the amount of provider vDC resources to allocate to the organization vDC.
- 5 [Allocate Storage](#) on page 30
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 31
You can provide a descriptive name and an optional description to indicate the vSphere functions available for your new organization vDC.
- 8 [Confirm Settings and Create the Organization vDC](#) on page 31
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. You can make a Pay-As-You-Go organization vDC elastic by adding multiple resource pools to its provider vDC.
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%.

Option	Action
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: Configuring an Allocation Model

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

Thin provisioning can help avoid over-allocating storage and save storage space. For a virtual machine with a thin virtual disk, ESX/ESXi provisions the entire space required for the disk's current and future activities. ESX/ESXi commits only as much storage space as the disk needs for its initial operations.

Fast provisioning saves time by using vSphere linked clones for certain operations. See “[Fast Provisioning of Virtual Machines](#),” on page 82.

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

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.
- 3 (Optional) Deselect the **Enable fast provisioning** check box to disable fast provisioning for virtual machines in the organization vDC.
- 4 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

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

Procedure

- 1 Type a name and optional description.
- 2 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, vCloud 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	<p>Accessible by multiple organizations. Virtual machines belonging to different organizations can connect to and see traffic on this network.</p> <p>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.</p>	External network
External organization network - NAT-routed connection	<p>Accessible only by this organization. Only virtual machines within this organization can connect to this network.</p> <p>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.</p>	External network and network pool
Internal organization network	<p>Accessible only by this organization. Only virtual machines within this organization can connect to and see traffic on this network.</p> <p>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.</p>	Network pool

Add an External Direct Organization Network

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

Prerequisites

Verify that you have an external network.

Procedure

- 1 Click the **Manage & Monitor** tab and 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 and click **Next**.

You can create an external direct organization network by 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. When you deselect this check box, you can select 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, which provides more control of what is accessible.

Prerequisites

Verify that you have an external network and a network pool.

Procedure

- 1 Click the **Manage & Monitor** tab and 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 and click **Next**.

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**.
- 5 (Optional) 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.

When you deselect this check box, you can select 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 settings 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 set how they are mapped. See [“Configure Port Forwarding for an Organization Network,”](#) on page 56.

Add an Internal Organization Network

You can add an internal organization network to which multiple vApps can connect and that only this organization can access.

Prerequisites

Verify that you have a network pool.

Procedure

- 1 Click the **Manage & Monitor** tab and 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 and click **Next**.

You can create an internal organization network by 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. When you deselect this check box, you can select an arbitrary network pool and later create an organization vDC that can access it.

- 5 Use the default network settings or type your own settings 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

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

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

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

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

This chapter includes the following topics:

- [“Enable Catalog Publishing,”](#) on page 35
- [“Create a Published Catalog,”](#) on page 36
- [“Upload a vApp Template,”](#) on page 36
- [“Import a vApp Template from vSphere,”](#) on page 37
- [“Upload a Media File,”](#) on page 37
- [“Import a Media File from vSphere,”](#) on page 38
- [“Publish a Catalog,”](#) on page 38

Enable Catalog Publishing

Before you can publish an organization's catalogs, you must enable catalog publishing for the organization.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Properties**.
- 3 On the **Catalog Publishing** tab, select **Allow publishing catalogs to all organizations** and click **OK**.

Create a Published Catalog

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

Prerequisites

Verify that you have an organization that allows catalog publishing.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click **Catalogs** and select **My Organization's Catalogs** in the left pane.
- 4 On the **Catalogs** tab, click **New**.
- 5 Type a catalog name and optional description and click **Next**.
- 6 Click **Next**.
- 7 Select **Publish to all organizations** and click **Next**.
- 8 Review the catalog settings and click **Finish**.

Upload a vApp Template

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

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

You can quarantine files that users upload to vCloud Director so that you can process the files before you accept them. For example, you can scan the files for viruses. See [“Quarantine Uploaded Files,”](#) on page 105.

Prerequisites

Verify that the following conditions exist:

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click **Catalogs** and select **My Organization's Catalogs** in the left pane.
- 4 On the **vApp Templates** tab, click **Upload**.
- 5 Click **Browse**, browse to the location of the OVF package, select it, and click **Open**.
- 6 Type a name and optional description for the vApp template.
- 7 Select an organization vDC and catalog and click **Upload**.

What to do next

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

Import a vApp Template from vSphere

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

Prerequisites

Verify that you are a vCloud Director system administrator.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click **Catalogs** and select **My Organization's Catalogs** in the left pane.
- 4 On the **vApp Templates** tab, click **Import from vSphere**.
- 5 Select a vCenter Server and a virtual machine.
- 6 Type a name and optional description for the vApp template.
- 7 Select an organization vDC and catalog.
- 8 Choose whether to move or copy the virtual machine to the catalog.
- 9 Choose whether to mark the vApp template as a Gold Master in the catalog.
If you mark a vApp template as a Gold Master, this information appears in the list of vApp templates.
- 10 Click **OK**.

What to do next

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

Upload a Media File

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

You can quarantine files that users upload to vCloud Director so that you can process the files before you accept them. For example, you might want to scan the files for viruses. See [“Quarantine Uploaded Files,”](#) on page 105.

Prerequisites

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click **Catalogs** and select **My Organization's Catalogs** in the left pane.
- 4 On the **Media** tab, click **Upload**.
- 5 Click **Browse**, browse to the location of the media file, select it, and click **Open**.
- 6 Type a name and optional description for the media file.
- 7 Select an organization vDC and catalog and click **Upload**.

Import a Media File from vSphere

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

Prerequisites

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click **Catalogs** and select **My Organization's Catalogs** in the left pane.
- 4 On the **Media** tab, click the **Import from vSphere** button.
- 5 Type a name and optional description for the media file.
- 6 Select the source vCenter Server and datastore and type the path to the media file.
- 7 Select an organization vDC and catalog.
- 8 Click **OK**.

Publish a Catalog

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

Prerequisites

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click **Catalogs** and select **My Organization's Catalogs** in the left pane.
- 4 On the Catalogs tab, right-click the catalog name and select **Publish**.
- 5 On the Publishing tab, select **Publish to all organizations** and click **OK**.

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

Managing Cloud Resources

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

This chapter includes the following topics:

- [“Managing Provider vDCs,”](#) on page 39
- [“Managing Organization vDCs,”](#) on page 43
- [“Managing External Networks,”](#) on page 49
- [“Managing Organization Networks,”](#) on page 50
- [“Managing Network Pools,”](#) on page 66
- [“Managing Cloud Cells,”](#) on page 67

Managing Provider vDCs

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

Enable or Disable a Provider vDC

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

When you disable a provider vDC, vCloud Director also disables the organization vDCs that use its resources. Running vApps and powered on virtual machines continue to run, but you cannot create or start additional vApps or virtual machines.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Provider vDCs** in the left pane.
- 2 Right-click the provider vDC name and select **Enable** or **Disable**.

Delete a Provider vDC

You can delete a provider vDC to remove its compute, memory, and storage resources from vCloud Director. The resources remain unaffected in vSphere.

Prerequisites

- Disable the provider vDC.

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

Procedure

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

Modify a Provider vDC Name and Description

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Provider vDCs** in the left pane.
- 2 Right-click the provider vDC name and select **Properties**.
- 3 Type a new name or description and click **OK**.

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

Enable or Disable a Provider vDC Host

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

To perform maintenance on a host, migrate all vApps off of the host or stop all vApps and then disable the host.

Procedure

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

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

Prepare or Unprepare a Provider vDC Host

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

For information about moving running virtual machines from one host to another, see [“Move Virtual Machines from one ESX/ESXi Host to Another,”](#) on page 71.

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

Prerequisites

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

Procedure

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

- 2 Right-click the provider vDC name and select **Open**.
- 3 Click the **Hosts** tab.
- 4 Right-click the host name and select **Prepare Host** or **Unprepare Host**.

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

Upgrade an ESX/ESXi Host Agent for a Provider vDC Host

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Provider vDCs** in the left pane.
- 2 Right-click the provider vDC name and select **Open**.
- 3 Click the **Hosts** tab.
- 4 Right-click the host name and select **Upgrade Host**.

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

Repair a Provider vDC ESX/ESXi Host

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Provider vDCs** in the left pane.
- 2 Right-click the provider vDC name and select **Open**.
- 3 Click the **Hosts** tab.
- 4 Right-click the host name and select **Repair Host**.

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

Enable 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**.

vCloud 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 **Add/Remove**.
- 5 Select a datastore from the list, click **Add**, and click **OK**.

vCloud 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 might appear. Do not add these datastores to your provider vDC.

Use only shared storage because vSphere DRS cannot migrate virtual machines on local storage.

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

Add a Resource Pool to a Provider vDC

You can add additional resource pools to a provider vDC so that pay-as-you-go organization vDCs that the provider vDC provides can expand.

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

Prerequisites

Verify that There is one or more available resource pool exists in the same vCenter datacenter as the provider vDC's primary resource pool.

Procedure

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

vCloud Director adds a resource pool for the provider vDC to use, making all pay-as-you-go organization vDCs backed by the provider vDC elastic.

Configure Low Disk Space Warnings for a Provider vDC Datastore

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Provider vDCs** in the left pane.
- 2 Right-click the provider vDC name and select **Open**.
- 3 Click the **Datastores** tab.
- 4 Right-click the datastore name and select **Properties**.
- 5 Select the disk space thresholds for the datastore.

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

- 6 Click **OK**.

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

Send an Email Notification to Provider vDC Users

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

Prerequisites

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Provider vDCs** in the left pane.
- 2 Right-click the provider vDC name and select **Notify**.
- 3 Type the email subject and message and click **Send Email**.

Managing Organization vDCs

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

Create an Organization vDC

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

Prerequisites

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

Procedure

- 1 [Open the New Organization vDC Wizard](#) on page 44
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 44
You can create an organization vDC to provide resources to any organization in the vCloud Director system. An organization can have more than one organization vDC.
- 3 [Select a Provider vDC](#) on page 44
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 45
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 45
Configure the allocation model to specify the amount of provider vDC resources to allocate to the organization vDC.
- 6 [Allocate Storage](#) on page 46
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 47
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 47

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

9 [Confirm Settings and Create the Organization vDC](#) on page 47

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 vCloud Director system. An organization can have more than one organization vDC.

Procedure

- 1 Select an organization.
- 2 Click **Next**.

Select a Provider vDC

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

Procedure

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

Select an Allocation Model

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

Procedure

- 1 Select an allocation model.

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. You can make a Pay-As-You-Go organization vDC elastic by adding multiple resource pools to its provider vDC.
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: Configuring an Allocation Model

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

Thin provisioning can help avoid over-allocating storage and save storage space. For a virtual machine with a thin virtual disk, ESX/ESXi provisions the entire space required for the disk's current and future activities. ESX/ESXi commits only as much storage space as the disk needs for its initial operations.

Fast provisioning saves time by using vSphere linked clones for certain operations. See [“Fast Provisioning of Virtual Machines,”](#) on page 82.

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

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.
- 3 (Optional) Deselect the **Enable fast provisioning** check box to disable fast provisioning for virtual machines in the organization vDC.
- 4 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

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

Procedure

- 1 Type a name and optional description.
- 2 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, vCloud Director creates a resource pool in vSphere to provide CPU and memory resources.

Enable or Disable an Organization vDC

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

Procedure

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

Delete an Organization vDC

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

Prerequisites

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

Procedure

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

Modify an Organization vDC Name and Description

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

Procedure

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

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

Edit Organization vDC Allocation Model Settings

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

Procedure

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

These settings only affect vApps that you start from this point on. vApps that are already running are not affected. The usage information that vCloud Director reports for this organization vDC 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 and fast provisioning for the organization vDC.

For information on fast provisioning, see [“Fast Provisioning of Virtual Machines,”](#) on page 82.

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**.

IMPORTANT Fast provisioning requires vCenter Server 5.0 and ESXi 5.0 hosts. If the provider vDC on which the organization vDC is based contains and ESX/ESXi 4.x hosts, you must disable fast provisioning.

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 vCloud Director installation grows, you might want to assign a more descriptive name or description to an existing external network.

Procedure

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

Modify an External Network Specification

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

Procedure

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

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

Add IP Addresses to an External Network IP Pool

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

Procedure

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

Delete an External Network

Delete an external network to remove it from vCloud Director.

Prerequisites

Before you can delete an external network, you must delete all of the 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	<p>Accessible by multiple organizations. Virtual machines belonging to different organizations can connect to and see traffic on this network.</p> <p>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.</p>	External network
External organization network - NAT-routed connection	<p>Accessible only by this organization. Only virtual machines within this organization can connect to this network.</p> <p>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.</p>	External network and network pool
Internal organization network	<p>Accessible only by this organization. Only virtual machines within this organization can connect to and see traffic on this network.</p> <p>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.</p>	Network pool

Create an External Direct Organization Network

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

Prerequisites

An external network.

Procedure

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

- 2 Click **Add Network**.

The Create Organization Network wizard starts.

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

- 4 Select the type of setup and network type and click **Next**.

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. When you deselect this check box, you can 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 better control on what is accessible.

Prerequisites

Verify that your organization has an external network and a network pool.

Procedure

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

- 2 Click **Add Network**.

The Create Organization Network wizard starts.

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

- 4 Select the type of setup and network type and click **Next**.

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. When you deselect this check box, you can choose an arbitrary network or network pool and later create an organization vDC that can access the network or network pool

- 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 available only 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 are mapped. See [“Configure Port Forwarding for an Organization Network,”](#) on page 56.

Create an Internal Organization Network

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

Prerequisites

Verify that you have a network pool.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organization Networks** in the left pane.
- 2 Click **Add Network**.
- 3 Select an organization and click **Next**.
- 4 Select the type of setup and network type and click **Next**.

You can create an internal 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. When you deselect this check box, you can 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, network address translation (NAT), and VPN for certain organization networks. Organization administrators can also configure some network services for their organization networks.

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

Table 5-5. Network Services Available by Network Type

Network Type	DHCP	Firewall	NAT	VPN
External organization network - direct connection				
External organization network - NAT-routed connection	X	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, vCloud 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.

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

- 5 Set the default lease time and maximum lease time or use the default values.
- 6 Click **OK**.

vCloud 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. You can enable the firewall on an organization network to enforce firewall rules on incoming traffic, outgoing traffic, or both.

You can deny all incoming traffic, deny all outgoing traffic, or both. You can also add specific firewall rules to allow or deny traffic that matches the rules to pass through the firewall. These rules take precedence over the generic rules to deny all incoming or outgoing traffic. See [“Add a Firewall Rule for an Organization Network,”](#) on page 54.

System administrators and organization administrators can enable firewalls.

Prerequisites

Verify that you have 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**.
- 4 Select the default firewall action.
- 5 (Optional) Select the **Log** check box to log events related to the default firewall action.
- 6 Click **OK**.

Add a Firewall Rule for an Organization Network

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

For a firewall rule to be enforced, you must enable the firewall for the organization network. See [“Enable the Firewall for an Organization Network,”](#) on page 54.

When you add a new firewall rule to an organization network, it appears at the bottom of the firewall rule list. For information about setting the order in which firewall rules are enforced, see [“Reorder Firewall Rules for an Organization Network,”](#) on page 55.

System administrators and organization administrators can add firewall rules.

Prerequisites

Verify that you have 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 Select the traffic direction.
- 6 Type the source IP address and select the source port.

For incoming traffic, the source is the external network. For outgoing traffic, the source is the organization network.

- 7 Type the destination IP address and select the destination port.
For incoming traffic, the destination is the organization network. For outgoing traffic, the destination is the external network.
- 8 Select the protocol.
- 9 Select the action.
A firewall rule can allow or deny traffic that matches the rule.
- 10 Select the **Enabled** check box.
- 11 (Optional) Select the **Log network traffic for firewall rule** check box.
If you enable this option, vCloud Director sends log events to the syslog server for connections affected by this rule. Each syslog message includes logical network and organization UUIDs.
- 12 Click **OK** and click **OK** again.

Reorder Firewall Rules for an Organization Network

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

When you add a new firewall rule to an organization network, it appears at the bottom of the firewall rule list. If you want to enforce the new rule before an existing rule, make sure to reorder the rules.

Prerequisites

A routed organization network with two or more firewall rules.

Procedure

- 1 Click **Administration**.
- 2 Select **Cloud Resources > Networks**.
- 3 Right-click the organization network name and select **Configure Services**.
- 4 Click the **Firewall** tab.
- 5 Drag and drop the firewall rules to establish the order in which the rules are applied.
- 6 Click **OK**.

Enable IP Masquerading for an Organization Network

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

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

Both system administrators and organization administrators can enable IP masquerade.

Prerequisites

Verify that you have 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 Mapping** tab and select **Enable IP Masquerade**.

- 4 Click **OK**.

Add External IP Addresses to an Organization Network

Before you can configure NAT 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 NAT mapping using the external IP address.

Configure Port Forwarding for an Organization Network

You can configure certain organization networks to provide port forwarding. Port forwarding provides external access to services running on virtual machines on the organization network.

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

When you add a new port forwarding rule to an organization network, it appears at the bottom of the NAT mapping rule list. For information about how to set the order in which NAT mapping rules are enforced, see [“Reorder NAT Mapping Rules for an Organization Network,”](#) on page 57.

Both system administrators and organization administrators can configure port forwarding.

Prerequisites

Verify that you have 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 Mapping** tab and click **Add**.
- 4 Select **Port Forwarding** and 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**.

Configure IP Translation for an Organization Network

You can configure certain organization networks to provide IP translation.

When you add a new IP translation rule to an organization network, it appears at the bottom of the NAT mapping rule list. For information about how to set the order in which NAT mapping rules are enforced, see [“Reorder NAT Mapping Rules for an Organization Network,”](#) on page 57.

When you create an IP translation rule for a network, vCloud Director adds a DNAT and SNAT rule to the vShield Edge associated with the network's port group. The DNAT rule translates an external IP address to an internal IP address for inbound traffic. The SNAT rule translates an internal IP address to an external IP address for outbound traffic. If the network is also using IP masquerade, the SNAT rule takes precedence.

Both system administrators and organization administrators can configure IP translation.

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 Mapping** tab and click **Add**.
- 4 Select **IP Translation** and configure the rule.
 - a Select an external IP address.
 - b 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 IP address.
 - c Click **OK**.
- 5 Click **OK**.

Reorder NAT Mapping Rules for an Organization Network

NAT mapping rules are enforced in the order in which they appear in the NAT mapping list. An organization administrator can change the order of the rules in the list.

When you add a new NAT mapping rule, such as IP translation or port forwarding, to an organization network, the rule appears at the bottom of the NAT mapping rule list. To enforce the new rule before an existing rule, reorder the rules.

Prerequisites

Verify that you have a routed organization network with two or more NAT mapping rules.

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 Mapping** tab.
- 4 Click and drag the rules to establish the order in which the rules are applied.
- 5 Click **OK**.

Enable Site-to-Site VPN for an Organization Network

You can enable site-to-site VPN for an organization network and then create a secure tunnel to another network.

vCloud Director supports site-to-site VPN between organization networks in the same organization, organization networks in different organizations (including organization networks in different instances of vCloud Director), and remote networks.

Both system administrators and organization administrators can enable site-to-site VPN.

Prerequisites

- An external NAT-routed organization network.
- vShield Manager 5.0.

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 **Site-to-Site VPN** tab and select **Enable site-to-site VPN**.
- 4 (Optional) Type a public IP address.

If the external network to which the organization network is routed is behind a NAT device, you must provide a publicly accessible IP address that faces the Internet.

- 5 Click **OK**.

What to do next

Create a VPN tunnel to another network.

Create a VPN Tunnel Within an Organization

You can create a VPN tunnel between two organizations networks in the same organization.

Both system administrators and organization administrators can create VPN tunnels.

If there is a firewall between the tunnel endpoints, you must configure it to allow the following IP protocols and UDP ports:

- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)
- UDP Port 500 (IKE)
- UDP Port 4500

Prerequisites

- At least two external NAT-routed organization networks with non-overlapping IP subnets and site-to-site VPN enabled on both networks.
- vShield Manager 5.0.

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 **Site-to-Site VPN** tab and click **Add**.
- 4 Type a name and optional description.
- 5 Select **a network in this organization** from the drop-down menu and select a peer network.
- 6 Review the tunnel settings and click **OK**.

vCloud Director configures both peer network endpoints.

Create a VPN Tunnel Between Organizations

You can create a VPN tunnel between two organizations networks in different organizations. The organizations can be part of the same vCloud Director installation or a different installation.

Both system administrators and organization administrators can create VPN tunnels.

If there is a firewall between the tunnel endpoints, you must configure it to allow the following IP protocols and UDP ports:

- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)
- UDP Port 500 (IKE)
- UDP Port 4500

Prerequisites

- An external NAT-routed organization network in each of the organizations. The organization networks must have non-overlapping IP subnets and site-to-site VPN enabled.
- vShield Manager 5.0.

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 **Site-to-Site VPN** tab and click **Add**.
- 4 Type a name and optional description.
- 5 Select **a network in another organization** from the drop-down menu.
- 6 Click **Connect to another organization**, type the login information for the peer organization, and click **Continue**.

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

- 7 Select a peer network.

8 Review the tunnel settings and click **Connect**.

vCloud Director configures both peer network endpoints.

Create a VPN Tunnel to a Remote Network

You can create a VPN tunnel between an organization network and a remote network.

Both system administrators and organization administrators can create VPN tunnels.

If there is a firewall between the tunnel endpoints, you must configure it to allow the following IP protocols and UDP ports:

- IP Protocol ID 50 (ESP)
- IP Protocol ID 51 (AH)
- UDP Port 500 (IKE)
- UDP Port 4500

Prerequisites

- An external NAT-routed organization network and a routed remote network that uses IPSec.
- vShield Manager 5.0.

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 **Site-to-Site VPN** tab and click **Add**.
- 4 Type a name and optional description.
- 5 Select a **remote network** from the drop-down menu.
- 6 Type the peer settings.
- 7 Review the tunnel settings and click **OK**.

vCloud Director configures the organization peer network endpoint.

What to do next

Manually configure the remote peer network endpoint.

Enable Static Routing for an Organization Network

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

Prerequisites

Verify that you have a 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 On the **Static Routing** tab, select **Enable static routing** and click **OK**.

What to do next

Create static routes. See [“Add Static Routes Between vApp Networks Routed to the Same Organization Network,”](#) on page 61 and [“Add Static Routes Between vApp Networks Routed to Different Organization Networks,”](#) on page 62.

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

You can add static routes between two vApp networks that are routed to the same organization network. Static routes allow traffic between the networks.

You cannot add static routes between overlapping networks or fenced vApps. After you add a static route to an organization network, configure the network firewall rules to allow traffic on the static route.

Static routes only function when the vApps included in the routes are running. If the vApp includes static routes and you change the parent network of a vApp, delete a vApp, or delete a vApp network, the static routes no longer function and you must remove them manually.

Prerequisites

Verify that the networks have the following configurations:

- vShield 5.0.
- A routed organization network.
- Static routing is enabled on the organization network.
- Two vApp networks are routed to the organization network.
- The vApp networks are in vApps that were started at least once.

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 On the **Static Routing** tab, click **Add**.

- 4 Type a name, network address, and next hop IP.

The network address is for the first vApp network to which you want to add a static route. The next hop IP is the external IP address of that vApp network's router.

- 5 Select **Within this network** and click **OK**.
- 6 Click **OK**.
- 7 Repeat steps [Step 3](#) through [Step 6](#) to add a route to the second vApp network.

Example: Static Routing Example

vApp Network 1 and vApp Network 2 are both routed to Org Network Shared. You can create static routes on the organization network to allow traffic between the vApp networks. You can use information about the vApp networks to create the static routes.

Table 5-6. Network Information

Network Name	Network Specification	Router External IP Address
vApp Network 1	192.168.1.0/24	192.168.0.100
vApp Network 2	192.168.2.0/24	192.168.0.101
Org Network Shared	192.168.0.0/24	NA

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

Table 5-7. Static Routing Settings

Static Route to Network	Route Name	Network	Next Hop IP Address	Route
vApp Network 1	tovapp1	192.168.1.0/24	192.168.0.100	Within this network
vApp Network 2	tovapp2	192.168.2.0/24	192.168.0.101	Within this network

What to do next

Create firewall rules to allow traffic on the static routes. See [“Add a Firewall Rule for an Organization Network,”](#) on page 54.

Add Static Routes Between vApp Networks Routed to Different Organization Networks

An organization administrator can add static routes between two vApp networks that are routed to different organization networks. Static routes allow traffic between the networks.

You cannot add static routes between overlapping networks or fenced vApps. After you add a static route to an organization network, configure the network firewall rules to allow traffic on the static route. For vApps with static routes, select the **Always use assigned IP addresses until this vApp or associated networks are deleted** check box.

Static routes only function when the vApps included in the routes are running. If a vApp includes static routes and you change the parent network of the vApp, delete the vApp, or delete a vApp network, the static routes cannot function and you must remove them manually.

Prerequisites

Verify that vCloud Director has the following configurations:

- vShield 5.0.
- Two organization networks routed to the same external network.
- Static routing is enabled on both organization networks.
- A vApp network is routed to each organization network.
- The vApp networks are in vApps that were started at least once.

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 On the **Static Routing** tab, click **Add**.
- 4 Type a name, network address, and next hop IP address.

The network address is for the vApp network to which you want to add a static route. The next hop IP address is the external IP address of the router for the organization network to which that vApp network is routed.

- 5 Select **To external network** and click **OK**.
- 6 Click **Add**.

- 7 Type a name, network address, and next hop IP address.

The network address is for the vApp network that is routed to this organization network. The next hop IP address is the external IP address of the router for that vApp network.

- 8 Select **Within this network** and click OK.
- 9 Repeat steps [Step 3](#) through [Step 8](#) to add static routes to the second organization network.

Example: Static Routing Example

vApp Network 1 is routed to Org Network 1. vApp Network 2 is routed to Org Network 2. You can create static routes on the organization networks to allow traffic between the vApp networks. You can use information about the vApp networks and organization networks to create the static routes.

Table 5-8. Network Information

Network Name	Network Specification	Router External IP Address
vApp Network 1	192.168.1.0/24	192.168.0.100
vApp Network 2	192.168.11.0/24	192.168.10.100
Org Network 1	192.168.0.0/24	10.112.205.101
Org Network 2	192.168.10.0/24	10.112.205.100

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

Table 5-9. Static Routing Settings for Org Network 1

Static Route to Network	Route Name	Network	Next Hop IP Address	Route
vApp Network 2	tovapp2	192.168.11.0/24	10.112.205.100	To external network
vApp Network 1	tovapp1	192.168.1.0/24	192.168.0.100	Within this network

Table 5-10. Static Routing Settings for Org Network 2

Static Route to Network	Route Name	Network	Next Hop IP Address	Route
vApp Network 1	tovapp1	192.168.1.0/24	10.112.205.101	To external network
vApp Network 2	tovapp2	192.168.11.0/24	192.168.10.100	Within this network

What to do next

Create firewall rules to allow traffic on the static routes. See [“Add a Firewall Rule for an Organization Network,”](#) on page 54.

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, you can reset the network.

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

No network services are available while an organization network resets.

Prerequisites

Verify that you have 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**.

View vApps and vApp Templates That Use an Organization Network

You can view a list of the all the vApps and vApp templates that include virtual machines with a NIC connected to an organization network. You cannot delete an organization network with connected vApps or vApp templates.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organization Networks** in the left pane.
- 2 Select an organization network, right-click, and select **Connected vApps**.
- 3 Click **OK**.

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. See [“View vApps and vApp Templates That Use an Organization Network,”](#) on page 64.

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**.

View IP Use for an Organization Network

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

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 vCloud 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**.

View Syslog Server Settings for an Organization Network

You can view the syslog server settings for a routed organization network.

vCloud Director supports logging events related to firewall rules to a syslog server that a system administrator specifies.

If an organization network lacks syslog server settings and you think that it should have them, or if the settings are not what you expected, synchronize the network with the most current syslog server settings. See [“Apply Syslog Server Settings to an Organization Network,”](#) on page 65.

Prerequisites

- Verify that you have an external NAT-routed organization network.
- Verify that you are an organization administrator.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organization Networks** in the left pane.
- 2 Select an organization network, right-click, and select **Properties**.
- 3 Click the **Syslog Server Settings** tab.

Apply Syslog Server Settings to an Organization Network

You can apply syslog server settings to a routed organization network to enable firewall rule logging.

Apply syslog server settings to any organization network that was created before the initial creation of those settings. Apply the syslog server settings to an organization network any time the settings are changed.

If you are unsure whether an organization network's syslog settings are up-to-date, you can view the organization network's syslog settings. See [“View Syslog Server Settings for an Organization Network,”](#) on page 65.

Prerequisites

Verify that you have an external NAT-routed organization network.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organization Networks** in the left pane.
- 2 Select an organization network, right-click, and select **Synchronize syslog server settings**.
- 3 Click **Yes**.

Managing Network Pools

After you create a network pool, you can modify its name or description or delete it. Depending on the type of network pool, you can also add port groups, Cloud isolated networks, and VLAN IDs.

Modify a Network Pool Name and Description

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

Procedure

- 1 Click the **Manage & Monitor** tab and then click **Network Pools** in the left pane.
- 2 Right-click the network pool name and select **Properties**.
- 3 On the **General** tab, type a new name or description and click **OK**.

Add a Port Group to a Network Pool

You can add port groups to a network pool that is backed by port groups.

Prerequisites

- Verify that you have a network pool that is backed by a port group
- Verify that you have an available port group in vSphere

Procedure

- 1 Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.
- 2 Right-click the network pool name and select **Properties**.
- 3 On the **Network Pool Settings** tab, select a port group, click **Add**, and click **OK**.

Add Cloud Isolated Networks to a Network Pool

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

Prerequisites

A VCD network isolation-backed network pool

Procedure

- 1 Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.
- 2 Right-click the network pool name and select **Properties**.

- 3 On the **Network Pool Settings** tab, type the number of VCD isolated networks and click **OK**.

Add VLAN IDs to a Network Pool

You can add VLAN IDs to a network pool that is backed by a VLAN.

Prerequisites

Verify that your system includes the following items:

- A network pool that is backed by a VLAN
- Available VLAN IDs in vSphere

Procedure

- 1 Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.
- 2 Right-click the network pool name and select **Properties**.
- 3 On the **Network Pool Settings** tab, type a VLAN ID range and click **Add**.
- 4 Select a vSphere distributed switch and click **OK**.

Delete a Network Pool

Delete a network pool to remove it from vCloud Director.

Prerequisites

Verify that the following conditions exist:

- No organization vDC is associated with the network pool.
- No vApps use the network pool
- No NAT-routed or internal organization networks use the network pool.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Network Pools** in the left pane.
- 2 Right-click the network pool name and select **Delete**.
- 3 Click **Yes**.

Managing Cloud Cells

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

[Table 5-11](#) lists the basic commands for controlling a cloud cell.

Table 5-11. Cloud Cell Commands

Command	Description
<code>service vmware-vcd start</code>	Starts the cell
<code>service vmware-vcd restart</code>	Restarts the cell
<code>service vmware-vcd stop</code>	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 68.

Adding Cloud Cells

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

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

Delete a Cloud Cell

If you want to remove a cloud cell from your vCloud Director installation, in order to reinstall the software, or for some other reason, you can delete the cell.

You can also delete a cell if it becomes unreachable.

Prerequisites

You must stop the cell using the `service vmware-vcd stop` command.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Cloud Cells** in the left pane.
- 2 Right-click the cell name and select **Delete**.

vCloud Director removes information about the cell from its database.

Turn On Cloud Cell Maintenance Message

If you want to stop a cell and let users know that you are performing maintenance, you can turn on the maintenance message.

When the maintenance message is turned on, users that attempt to log in to the cell from browser will see a message stating that the cell is down for maintenance. Users 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

After you add vSphere resources to the vCloud Director system, you can perform some management functions from vCloud Director. You can also use the vSphere Client to manage these resources.

vSphere resources include vCenter servers, resource pools, ESX/ESXi hosts, datastores, and network switches and ports.

This chapter includes the following topics:

- [“Managing vSphere vCenter Servers,”](#) on page 69
- [“Managing vSphere ESX/ESXi Hosts,”](#) on page 71
- [“Managing vSphere Datastores,”](#) on page 72
- [“Managing Stranded Items,”](#) on page 73

Managing vSphere vCenter Servers

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

Register vCloud Director with a vCenter Server

You can register vCloud Director with the vCenter Servers it uses.

After you register vCloud Director, it appears as an extension in the vSphere Client Solutions Manager tab. In addition, the vSphere Client sets the **Managed By** property for vCloud Director-managed virtual machines, which protects those virtual machines from being modified using the vSphere Client.

Procedure

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

Modify vCenter Server Settings

If the connection information for a vCenter Server changes, or if you want to change how its name or description appears in vCloud Director, you can modify its settings.

Procedure

- 1 Click the **Manage & Monitor** tab and click **vCenters** in the left pane.
- 2 Right-click the vCenter Server name and select **Properties**.

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

Reconnect a vCenter Server

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

Procedure

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

Enable or Disable a vCenter Server

You can disable a vCenter Server to perform maintenance.

Procedure

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

Remove a vCenter Server

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

Prerequisites

Before you can remove a vCenter server, you must disable it and delete all of the provider vDCs that use its resource pools.

Procedure

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

Prepare and Upgrade a vCenter Server Attached to vCloud Director

Before you upgrade a vCenter Server that is attached to vCloud director, you must prepare the server by disabling it in vCloud Director.

Familiarize yourself with the *vSphere Upgrade* documentation.

Procedure

- 1 In the vCloud Director web console, click the **Manage & Monitor** tab and click **vCenters** in the left pane.
- 2 Right-click the vCenter Server name and select **Disable**.
- 3 Click **Yes**.
- 4 Upgrade vCenter Server.
- 5 In the vCloud Director web console, right-click the vCenter Server name and select **Enable**.
- 6 Click **Yes**.

What to do next

Register vCloud Director with the upgraded server. See [“Register vCloud Director with a vCenter Server,”](#) on page 69.

Modify vShield Manager Settings

If the connection settings for the vShield Manager for a vCenter Server change, or if you want to use a different vShield Manager, you can modify its settings.

Procedure

- 1 Click the **Manage & Monitor** tab and click **vCenters** in the left pane.
- 2 Right-click the vCenter Server name and select **Properties**.
- 3 On the **vShield Manager** tab, type the new settings and click **OK**.

Managing vSphere ESX/ESXi Hosts

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

Enable or Disable an ESX/ESXi Host

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

To perform maintenance on a host, migrate all vApps off of the host or stop all vApps and then disable the host.

Procedure

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

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

Move Virtual Machines from one ESX/ESXi Host to Another

You can move all the virtual machines from one ESX/ESXi host to other hosts in the same cluster. This ability is useful to unprepare a host, or to perform maintenance on a host without affecting running virtual machines.

Prerequisites

Disable the host.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Hosts** in the left pane.
- 2 Right-click the host name and select **Redeploy all VMs**.
- 3 Click **Yes**.

vCloud Director puts the host into maintenance mode and moves all of its virtual machines to other hosts in the same cluster.

Prepare or Unprepare an ESX/ESXi Host

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

For information about moving virtual machines from one host to another, see [“Move Virtual Machines from one ESX/ESXi Host to Another,”](#) on page 71.

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

Prerequisites

Disable the host and ensure that no virtual machines are running on the host.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Hosts** in the left pane.
- 2 Right-click the host name and select **Prepare Host** or **Unprepare Host**.
- 3 If you are preparing a host, type a user name and password and click **OK**.

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

Upgrade an ESX/ESXi Host Agent

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

Procedure

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

Repair an ESX/ESXi Host

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

Procedure

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

Managing vSphere Datastores

You can enable or disable vSphere datastores in the vCloud Director system, configure low disk space warnings for datastores, and remove datastores from the vCloud Director system.

The only way to add a datastore to vCloud Director is to add it to a provider vDC. See [“Add Storage Capacity to a Provider vDC,”](#) on page 41.

Enable or Disable a Datastore

You can enable or disable a datastore that has been added to a provider vDC. You must disable a datastore before you can remove it from vCloud Director.

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Datastores** in the left pane.
- 2 Right-click the datastore name and select **Enable** or **Disable**.

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

Remove a Datastore

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

Prerequisites

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

Procedure

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

vCloud Director removes the datastore.

Configure Low Disk Space Warnings for a Datastore

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Datastores** in the left pane.
- 2 Right-click the datastore name and select **Properties**.
- 3 On the **General** tab, select the disk space thresholds for the datastore.

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

- 4 Click **OK**.

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

Managing Stranded Items

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

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

Delete a Stranded Item

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Stranded Items** in the left pane.

- 2 Right-click a stranded item and select **Delete**.
- 3 Click **Yes**.

vCloud Director attempts to delete the stranded item from vSphere.

- 4 Refresh the page display.

If the delete operation is successful, vCloud Director removes the item from the stranded items list.

What to do next

If the delete operation is unsuccessful, you can force delete the item. See [“Force Delete a Stranded Item,”](#) on page 74.

Force Delete a Stranded Item

If vCloud Director cannot delete a stranded item, you can force delete it to remove it from the stranded items list. The stranded item continues to exist in vSphere.

Before you force delete a stranded item, try to delete it. See [“Delete a Stranded Item,”](#) on page 73.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Stranded Items** in the left pane.
- 2 Right-click a stranded item and select **Force Delete**.
- 3 Click **Yes**.

vCloud Director removes the item from the stranded items list.

Managing Organizations

After you create an organization, you can modify its properties, enable or disable it, or delete it.

This chapter includes the following topics:

- [“Enable or Disable an Organization,”](#) on page 75
- [“Delete an Organization,”](#) on page 75
- [“Modify an Organization Name,”](#) on page 76
- [“Modify an Organization Full Name and Description,”](#) on page 76
- [“Modify Organization LDAP Options,”](#) on page 76
- [“Modify Organization Catalog Publishing Policy,”](#) on page 77
- [“Modify Organization Email Preferences,”](#) on page 78
- [“Modify Organization Lease, Quota, and Limit Settings,”](#) on page 78
- [“Add a Catalog to an Organization,”](#) on page 79
- [“Managing Organization Resources,”](#) on page 79
- [“Managing Organization Users and Groups,”](#) on page 80
- [“Managing Organization vApps and Virtual Machines,”](#) on page 80

Enable or Disable an Organization

Disabling an organization prevents users from logging in to the organization and terminates the sessions of currently logged in users. Running vApps in the organization continue to run.

A system administrator can allocate resources, add networks, and so on, even after an organization is disabled.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Enable** or **Disable**.

Delete an Organization

Delete an organization to permanently remove it from vCloud Director.

Prerequisites

Before you can delete an organization, you must disable it and delete or change ownership of all objects that the organization users own.

Procedure

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

Modify an Organization Name

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

Prerequisites

You must disable the organization before you can rename it.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Properties**.
- 3 On the **General** tab, type a new organization name and click **OK**.

The internal organization URL changes to reflect the new name.

Modify an Organization Full Name and Description

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Properties**.
- 3 On the **General** tab, type a new full name or description and click **OK**.

Modify Organization LDAP Options

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

For more information about entering custom LDAP settings, see [“Configuring the System LDAP Settings,”](#) on page 93.

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 vCloud 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 vCloud Director installation.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Properties**.
- 3 Click the **Catalog Publishing** tab.
- 4 Select a catalog publishing option and click **OK**.

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

vCloud Director requires an SMTP server to send user notification and system alert emails. You can modify the settings you specified when you created the organization.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Properties**.
- 3 Click the **Email Preferences** tab.
- 4 Select an SMTP server option.

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 acts as a default for all new users added to the organization.

- 6 Select the limits for resource intensive operations.

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

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

Add a Catalog to an Organization

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

Prerequisites

Verify that you have an organization in which to create a catalog.

Procedure

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

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

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

Managing Organization Resources

vCloud Director organizations obtain their resources for one or more organization vDCs. If an organization needs more resources, you can add a new organization vDC or modify an existing organization vDC. You can take resources away from an organization by removing or modifying an organization vDC.

For more information about adding an organization vDC, see [“Create an Organization vDC,”](#) on page 43.

For information about removing an organization vDC, see [“Delete an Organization vDC,”](#) on page 47.

For information about modifying the resources available to an existing organization vDC, see [“Edit Organization vDC Allocation Model Settings,”](#) on page 48, and [“Edit Organization vDC Storage Settings,”](#) on page 48.

Managing Organization Users and Groups

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

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

Managing Organization vApps and Virtual Machines

Some tasks related to managing organization vApps and virtual machines can only be performed by a system administrator. For example, system administrators can add vSphere virtual machines to an existing vApp, create a vApp based on a vSphere virtual machine, and place a vApp in maintenance mode.

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

Add a vSphere Virtual Machine to a vApp

A system administrator can import a vSphere virtual machine into an existing vCloud Director vApp.

Prerequisites

You must be logged in to vCloud Director as a system administrator and the organization containing the vApp must have an available organization vDC.

Procedure

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

Create a vApp Based on a vSphere Virtual Machine

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

Prerequisites

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

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click the **My Cloud** tab and click **vApps** in the left pane.

- 4 Click **Import from vSphere**.
- 5 Select a vCenter Server and a virtual machine.
- 6 Type a name and optional description for the vApp and select a destination organization vDC.
- 7 Select whether to copy or move the source virtual machine.
- 8 Click **OK**.

Place a vApp in Maintenance Mode

A system administrator can place a vApp in maintenance mode to prevent non-administrator users from changing the state of the vApp. This is useful, for example, when you want to back up a vApp using a third-party backup solution.

When a vApp is in maintenance mode, non-system administrator users cannot perform any actions that modify the state of the vApp or its virtual machine. They can view information about the vApp and its virtual machines and access the virtual machine consoles.

Placing a vApp in maintenance mode does not affect any currently running tasks that involve the vApp.

Prerequisites

You must be logged in to vCloud Director as a system administrator.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click the **My Cloud** tab and click **vApps** in the left pane.
- 4 Right-click the vApp name and select **Enter Maintenance Mode**.
- 5 Click **Yes**.

The status of the vApp changes to **In Maintenance Mode**. The vApp remains in maintenance mode until you select **Exit Maintenance Mode**.

Force Stop a Running vApp

A system administrator can force stop a running vApp when an organization user is unable to do so.

In some cases, a user may be unable to stop a running vApp. If traditional methods for stopping the vApp fail, you can force stop the vApp to prevent the user from getting billed.

Force stopping a vApp does not prevent the vApp from consuming resources in vSphere. After you force stop a vApp in vCloud Director, use the vSphere Client to check the status of the vApp in vSphere and take the necessary action.

Prerequisites

You must be logged in to vCloud Director as a system administrator.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click the **My Cloud** tab and click **vApps** in the left pane.
- 4 Right-click the running vApp and select **Force Stop**.
- 5 Click **Yes**.

Fast Provisioning of Virtual Machines

Fast provisioning saves time by using linked clones for virtual machine provisioning operations.

A linked clone is a duplicate of a virtual machine that uses the same base disk as the original, with a chain of delta disks to track the differences between the original and the clone. If fast provisioning is disabled, all provisioning operations result in full clones.

A linked clone cannot exist on a different vCenter datacenter or datastore than the original virtual machine. vCloud Director creates shadow virtual machines to support linked clone creation across vCenter datacenters and datastores for virtual machines associated with a vApp template. A shadow virtual machine is an exact copy of the original virtual machine. The shadow virtual machine is created on the datacenter and datastore where the linked clone is created. You can view a list of shadow virtual machines associated with a template virtual machine. See [“View Shadow Virtual Machines Associated With a Virtual Machine,”](#) on page 82.

Fast provisioning is enabled by default on organization vDCs. Fast provisioning requires vCenter 5.0 and ESXi 5.0 hosts. If the provider vDC on which the organization vDC is based contains ESX/ESXi 4.x hosts, you must disable fast provisioning. See [“Edit Organization vDC Storage Settings,”](#) on page 48.

View Shadow Virtual Machines Associated With a Virtual Machine

Shadow virtual machines support linked clones of virtual machines that are associated with vApp templates across vCenter datacenters and datastores.

A shadow virtual machine is an exact copy of the original virtual machine that vCloud Director creates on the datacenter and datastore where a linked clone is created. See [“Fast Provisioning of Virtual Machines,”](#) on page 82.

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 **VMs** in the left pane.
- 4 Right-click the virtual machine and select **Properties**.
- 5 Click the **Shadow VMs** tab.

This tab appears only for virtual machines that have associated shadow virtual machines.

vCloud Director shows a list of shadow virtual machines associated with the virtual machine. This list includes the name in vCenter of each shadow virtual machine, the datastore that each shadow virtual machine exists on, and the vCenter server that the shadow virtual machine belongs to.

Managing System Administrators and Roles

8

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

This chapter includes the following topics:

- [“Add a System Administrator,”](#) on page 83
- [“Import a System Administrator,”](#) on page 84
- [“Enable or Disable a System Administrator,”](#) on page 84
- [“Delete a System Administrator,”](#) on page 84
- [“Edit System Administrator Profile and Contact Information,”](#) on page 84
- [“Send an Email Notification to Users,”](#) on page 85
- [“Delete a System Administrator Who Lost Access to the System,”](#) on page 85
- [“Import an LDAP Group,”](#) on page 85
- [“Delete an LDAP Group,”](#) on page 86
- [“Change an LDAP Group Description,”](#) on page 86
- [“Roles and Rights,”](#) on page 86
- [“Create a Role,”](#) on page 86
- [“Copy a Role,”](#) on page 87
- [“Edit a Role,”](#) on page 87
- [“Delete a Role,”](#) on page 87

Add a System Administrator

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

Procedure

- 1 Click the **Administration** tab and click **Users** in the left pane.
- 2 Click **New**.
- 3 Type the account information for the new user and click **OK**.

Import a System Administrator

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

Prerequisites

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

Procedure

- 1 Click the **Administration** tab and click **Users** in the left pane.
- 2 Click **Import from LDAP**.
- 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 vCloud Director. To delete a system administrator, you must first disable their account.

Procedure

- 1 Click the **Administration** tab and click **Users** in the left pane.
- 2 Right-click the user name and select **Enable Account** or **Disable Account**.

Delete a System Administrator

You can remove a system administrator from the vCloud Director system by deleting their account.

Prerequisites

Disable the system administrator account.

Procedure

- 1 Click the **Administration** tab and click **Users** in the left pane.
- 2 Right-click the user name and select **Delete**.
- 3 Click **Yes**.

Edit System Administrator Profile and Contact Information

You can change the password and contact information for a system administrator account.

You can only edit account information for 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 users in the entire installation, all system administrators, or all organization administrators. You can send an email notification to notify users about upcoming system maintenance, for example.

Prerequisites

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

Procedure

- 1 Click the **Administration** tab and click **Users** in the left pane.
- 2 Click **Notify**.
- 3 Select the recipients.
- 4 Type the email subject and message and click **Send Email**.

Delete a System Administrator Who Lost Access to the System

You can view a list of user accounts that lost access to the system when their LDAP group was deleted from vCloud Director. You can decide whether or not to add the user back into the system and then delete the user from the **Lost & Found**.

To add a user that was mistakenly removed from the system when their LDAP group was deleted, see [“Add a System Administrator,”](#) on page 83 and [“Import a System Administrator,”](#) on page 84.

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 vCloud 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 **Import from LDAP**.
- 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 vCloud Director system by deleting their LDAP group.

When you delete an LDAP group, users who have a vCloud Director account based solely on their membership in that group are stranded and cannot log in. See [“Delete a System Administrator Who Lost Access to the System,”](#) on page 85.

Procedure

- 1 Click the **Administration** tab and click **Groups** in the left pane.
- 2 Right-click the group name and select **Delete**.
- 3 Click **Yes** to confirm the deletion.

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

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

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

For information about the predefined roles and their rights, see [“Predefined Roles and Their Rights,”](#) on page 107.

Create a Role

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

Procedure

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

Copy a Role

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

Procedure

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

Edit a Role

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

Procedure

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

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

Delete a Role

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

Prerequisites

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

Procedure

- 1 Click the **Administration** tab and click **Roles** in the left pane.
- 2 Right-click a role and select **Delete**.
- 3 Click **Yes** to confirm the deletion.

Managing System Settings

A vCloud Director system administrator can control system-wide settings related to LDAP, email notification, licensing, and general system preferences.

This chapter includes the following topics:

- [“Modify General System Settings,”](#) on page 89
- [“General System Settings,”](#) on page 90
- [“Configure SMTP Settings,”](#) on page 91
- [“Configure System Notification Settings,”](#) on page 91
- [“Configuring Blocking Tasks and Notifications,”](#) on page 92
- [“Configuring the System LDAP Settings,”](#) on page 93
- [“Customize the vCloud Director Client UI,”](#) on page 96
- [“Configure the Public Web URL,”](#) on page 97
- [“Configure the Public Console Proxy Address,”](#) on page 98
- [“Configure the Public REST API Base URL,”](#) on page 98
- [“Configure the Account Lockout Policy,”](#) on page 98

Modify General System Settings

vCloud Director includes general system settings related to login policy, session timeouts, and so on. The default settings are appropriate for many environments, but you can modify the settings to meet your needs.

For more information, see [“General System Settings,”](#) on page 90.

Procedure

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

General System Settings

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

Table 9-1. General System Settings

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 synchronisations.
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 vCloud Director task log.
IP address release timeout	Networking	Number of seconds to keep released IP addresses on hold before making them available for allocation again. This default setting is 2 hours (7200 seconds) to allow old entries to expire from client ARP tables.
Allow Overlapping External Networks	Networking	Select the check box to add external networks that run on the same network segment. Enable this setting only if you are using non-VLAN-based methods (for example, VMware vShield Manager) to isolate your external networks.
Default syslog server settings for networks	Networking	Type IP addresses for up to two Syslog servers for networks to use. This setting does not apply to Syslog servers used by cloud cells.
Provider Locale	Localization	Select a locale for provider activity, including log entries, email alerts, and so on.
Idle session timeout	Miscellaneous	Amount of time the vCloud Director application remains active without user interaction.
Maximum session timeout	Miscellaneous	Maximum amount of time the vCloud Director application remains active.
Host refresh frequency	Miscellaneous	How often vCloud 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.
Transfer session timeout	Miscellaneous	Amount of time to wait before failing a paused or canceled upload task, for example upload media or upload vApp template. This timeout does not affect upload tasks that are in progress.
Chargeback Event History to Keep	Miscellaneous	Number of days of chargeback event history to keep before deleting it.
Chargeback Event Cleanup Start Time	Miscellaneous	Time of day to start chargeback event history cleanup.
Provide default vApp names	Miscellaneous	Select the check box to generate default names for vApps.

Table 9-1. General System Settings (Continued)

Name	Category	Description
Enable upload quarantine with a timeout of __ seconds	Miscellaneous	Select the check box and enter a timeout number representing the amount of time to quarantine uploaded files. For more information about working with quarantined files, see “Monitoring Quarantined Files,” on page 105.
Verify vCenter certificates	Miscellaneous	Select the check box to allow vCloud Director to communicate only with trusted vCenter servers. Click Browse to locate the JCEKS keystore and type the keystore password.

Configure SMTP Settings

vCloud Director requires an SMTP server to send user notifications and system alert emails to system users. Organizations can use the system SMTP settings, or use custom SMTP settings.

Procedure

- 1 Click the **Administration** tab and click **Email** in the left pane.
- 2 Type the DNS host name or IP address of the SMTP mail server.
- 3 Type the SMTP server port number.
- 4 (Optional) If the SMTP server requires a user name, select the **Requires authentication** check box and type the user name and password for the SMTP account.
- 5 Type an email address to appear as the sender for vCloud Director emails.
vCloud Director uses the sender's email address to send runtime and storage lease expiration alerts.
- 6 Type text to use as the subject prefix for vCloud Director emails.
- 7 (Optional) Type a destination email address to test the SMTP settings and click **Test SMTP settings**.
- 8 Click **Apply**.

Configure System Notification Settings

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

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

Prerequisites

A valid connection to an SMTP server.

Procedure

- 1 Click the **Administration** tab and click **Email** in the left pane.
- 2 Select the recipients of system alert emails and click **Apply**.

Configuring Blocking Tasks and Notifications

Blocking tasks and notifications allow a system administrator to configure vCloud Director to send AMQP messages triggered by certain events.

Some of these messages are simply notifications that the event has occurred. These are known as notifications. Others publish information to a designated AMQP endpoint indicating that a requested action has been blocked pending action by a client program bound to that endpoint, and are known as blocking tasks.

A system administrator can configure a system-wide set of blocking tasks that are subject to programmatic action by an AMQP client.

Configure an AMQP Broker

You must configure an AMQP broker if you want vCloud Director to send AMQP messages triggered by certain events.

Procedure

- 1 Click the **Administration** tab and click **Blocking Tasks** in the left pane.
- 2 Click the **Settings** tab.
- 3 Type the DNS host name or IP address of the AMQP host.
Type the AMQP port.
The default port is **5672**.
- 4 Type the exchange.
- 5 Type the vHost.
- 6 To use SSL, select the SSL check box and choose one of the certificate options.

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

- 7 Type a user name and password to connect to the AMQP host.
- 8 Click **Test AMQP Connection** to test the settings.
- 9 Click **Apply**.
- 10 (Optional) Select the **Enable Notifications** check box at the top of the page to publish audit events to the AMQP broker.

Configure Blocking Task Settings

You can specify status text, timeout settings, and default actions for blocking tasks. The settings apply to all organizations in the installation.

Procedure

- 1 Click the **Administration** tab and click **Blocking Tasks** in the left pane.
- 2 Click the **Settings** tab.
- 3 Type the text to appear as the status of a task that is pending extension processing.
- 4 Select the default extension timeout.

- 5 Select the default timeout action.
- 6 Click **Apply**.

Enable Blocking Tasks

You can configure certain tasks to be enabled for blocking tasks.

Procedure

- 1 Click the **Administration** tab and click **Blocking Tasks** in the left pane.
- 2 Click the **Blocking Tasks** tab.
- 3 Select the tasks to enable for blocking extensions
- 4 Click **Apply**.

Configuring the System LDAP Settings

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

After you connect vCloud Director to an LDAP server, you can import system administrators from the groups and users in the LDAP directory. You can also use the system LDAP settings to import users and groups to an organization, or you can specify separate LDAP settings for each organization. An LDAP user cannot log in to vCloud Director until you import them to the system or an organization.

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

vCloud Director does not support hierarchical domains for LDAP authentication.

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

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

LDAP Support

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

[Table 9-2](#) displays a list of what vCloud Director supports.

Table 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
Windows 7 (2008 R2)	Active Directory	Kerberos SSL

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

Operating System	LDAP Server	Authentication Method
Linux	OpenLDAP	Simple
Linux	OpenLDAP	Simple SSL

Configure an LDAP Connection

You can configure an LDAP connection to provide vCloud Director and its organizations with access to users and groups on the LDAP server.

Prerequisites

In order to use Kerberos as your authentication method, you must add a realm. See [“Add a Kerberos Realm,”](#) on page 95.

Procedure

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

- 2 Type the host name or IP address of the LDAP server.

For Kerberos authentication, use the fully qualified domain name (FQDN).

- 3 Type a port number.

For LDAP, the default port number is 389. For LDAP over SSL (LDAPS), the default port number is 636.

- 4 Type the base distinguished name (DN).

The base DN is the location in the LDAP directory where vCloud Director connects. VMware recommends connecting at the root. Type the domain components only, for example, **DC=example, DC=com**.

To connect to a node in the tree, type the distinguished name for that node, for example, **OU=ServiceDirector, DC=example, DC=com**. Connecting to a node limits the scope of the directory available to vCloud Director.

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

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

- 6 Select an authentication method.

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

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

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

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

- 8 Click **Apply**.

What to do next

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

Add a Kerberos Realm

vCloud Director requires a realm to use Kerberos authentication for an LDAP connection. You can add one or more realms for the system and its organizations to use. The system and each organization can only specify a single realm.

Prerequisites

You must select Kerberos as the authentication method before you can add a realm.

Procedure

- 1 Click the **Administration** tab and click **LDAP** in the left pane.
- 2 Click **Edit All Realms**.
- 3 (Optional) On the **Realm** tab, select **Allow lower-case realms** to allow realm names that include lower-case letters.
- 4 On the **Realm** tab, click **Add**.
- 5 Type a realm and its Key Distribution Center (KDC) and click **OK**.
If you did not choose to allow lower-case realms, the realm name must be all capital letters. For example, **REALM**.
- 6 On the **DNS** tab, click **Add**.
- 7 Type a DNS, select a realm, and click **OK**.
You can use the period (.) as a wildcard character in the DNS. For example, type **.example.com**.
- 8 Click **Close** and click **Apply**.

What to do next

You can now select a realm for the system LDAP settings or an organization's LDAP settings.

Test LDAP Settings

After you configure an LDAP connection, you can test its settings to make sure that user and group attributes are mapped correctly.

Prerequisites

You must configure an LDAP connection before you can test it.

Procedure

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

- 2 Click **Test LDAP Settings**.
- 3 Type the name of a user in the LDAP directory and click **Test**.
- 4 Review the attribute mapping and click **OK**.

What to do next

You can customize LDAP user and group attributes based on the results of the test.

Customize LDAP User and Group Attributes

LDAP attributes provide vCloud Director with details about how user and group information is defined in the LDAP directory. vCloud Director maps the information to its own database. Modify the syntax for user and group attributes to match your LDAP directory.

Prerequisites

Verify that you have an LDAP connection

Procedure

- 1 Click the **Administration** tab and click **LDAP** in the left pane.
- 2 Modify the user and group attributes and click **Apply**.

Synchronize vCloud Director with the LDAP Server

vCloud Director automatically synchronizes its user and group information with the LDAP server on a regular basis. You can also manually synchronize with the LDAP server at any time.

For automatic synchronization, you can specify how often and when to synchronize. See [“Modify General System Settings,”](#) on page 89.

Prerequisites

Verify that you have a valid LDAP connection.

Procedure

- 1 Click the **Administration** tab and click **LDAP** in the left pane.
- 2 Click **Synchronize LDAP**.

Customize the vCloud Director Client UI

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

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

vCloud Director uses its default logo, or the logo that you upload, in the login screen, the header, and the footer. The login screen shows the logo in an area that ranges from a minimum of 48x48 pixels to a maximum of 60x150 pixels. You can upload logos that are smaller than 48x48 or larger than 60x150 and vCloud Director scales them to fit in the display area and maintain the aspect ratio of the uploaded image. The file size for an uploaded image cannot exceed 16384 bytes. The header and footer scale the logo to an appropriate size and maintain the aspect ratio of the original.

The file must be in the PNG, JPEG, or GIF format.

Procedure

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

- 2 Type a company name.
This name appears in the title bar for system administrators and in the footer for all users.
- 3 To select a custom logo, click **Browse**, select a file, and click **Open**.
- 4 To select a custom theme, click **Browse**, select a .css file, and click **Open**.
- 5 Type a URL that links to a Web site that provides information about your vCloud Director installation.
For example, <http://www.example.com>. Users can follow the link by clicking the company name in the footer of the client UI.
- 6 Type a URL that links to a Web site that provides support for this vCloud Director installation.
The **Support** link on the **Home** tab of all vCloud Director organizations opens this URL.
- 7 Type a URL that links to a Web site that allows users to sign up for a vCloud Director account.
This link appears on the vCloud Director login page.
- 8 Type a URL that links to a Web site that allows users to recover their password.
This link appears on the vCloud Director login page.
- 9 Click **Apply**.

Revert to System Default Logo

If you uploaded a custom logo for vCloud Director, you can revert to the system default logo.

Prerequisites

Verify that you uploaded a custom logo.

Procedure

- 1 Click the **Administration** tab and click **Branding** in the left pane.
- 2 Select **Revert back to system default logo** and click **Apply**.

Revert to System Default Theme

If you applied a custom theme to vCloud Director, you can always revert to the system default theme.

Prerequisites

Verify that you previously applied a custom theme.

Procedure

- 1 Click the **Administration** tab and click **Branding** in the left pane.
- 2 Select **Revert back to system default theme** and click **Apply**.

Configure the Public Web URL

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

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

Procedure

- 1 Click the **Administration** tab and click **Public Addresses** in the left pane.

- 2 Type the public web URL.
- 3 Click **Apply**.

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

Configure the Public Console Proxy Address

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

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

Procedure

- 1 Click the **Administration** tab and click **Public Addresses** in the left pane.
- 2 Type the hostname or IP address for the public console proxy address.

This can be the address of the load balancer or some other machine that can route traffic to the remote console proxy IP.

- 3 Click **Apply**.

Remote console session tickets sent to the HTTP service IP address return the public console proxy address.

Configure the Public REST API Base URL

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

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

Procedure

- 1 Click the **Administration** tab and click **Public Addresses** in the left pane.
- 2 Type the hostname or IP address for the public REST API base URL.

This can be the address of the load balancer or some other machine that can route traffic to the HTTP service IP.

- 3 Click **Apply**.

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

Configure the Account Lockout Policy

You can enable account lockout to prevent a user from logging in to the Web console after a certain number of failed attempts. By default, the settings you specify apply to all organizations in the installation, but a system administrator or organization administrator can override the settings for a specific organization.

Procedure

- 1 Click the **Administration** tab and click **Password Policy** in the left pane.

- 2 Select the **Account lockout enabled** check box, the **System Administrator account can lockout** check box, or both.
- 3 Select the number of invalid logins to accept before locking an account.
- 4 Select the lockout interval.
- 5 Click **Apply**.

Monitoring vCloud Director

System administrators can monitor completed and in-progress operations and view resource usage information at the provider vDC, organization vDC, and datastore level.

This chapter includes the following topics:

- [“Viewing Tasks and Events,”](#) on page 101
- [“Monitor and Manage Blocking Tasks,”](#) on page 103
- [“View Usage Information for a Provider vDC,”](#) on page 103
- [“View Usage Information for an Organization vDC,”](#) on page 103
- [“Using vCloud Director's JMX Service,”](#) on page 104
- [“Viewing the vCloud Director Logs,”](#) on page 104
- [“vCloud Director and Cost Reporting,”](#) on page 104
- [“Monitoring Quarantined Files,”](#) on page 105

Viewing Tasks and Events

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

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

vCloud Director events represent one-time occurrences that typically indicate an important part of an operation or a significant state change for a vCloud Director object. For example, vCloud Director logs an event when a user initiates the creation an organization vDC and another event when the process completes. vCloud Director also logs an event every time a user logs in and notes whether the attempt was successful or not.

View Ongoing and Completed System Tasks

View the system log to monitor system-level tasks that are in progress, to find and troubleshoot failed tasks, and to view tasks by owner.

To view information about organization-level tasks, see [“View Ongoing and Completed Organization Tasks,”](#) on page 102.

The log can also include debug information, depending on your vCloud Director settings. See [“General System Settings,”](#) on page 90.

Procedure

- 1 Log in to the vCloud Director system as a system administrator.
- 2 Click the **Manage & Monitor** tab and click **Logs** in the left pane.
- 3 Click the **Tasks** tab.
vCloud Director displays information about each system-level task.
- 4 Double-click a task for more information.

View Ongoing and Completed Organization Tasks

View the log for an organization to monitor organization-level tasks that are in progress, to find and troubleshoot failed tasks, and to view tasks by owner.

To view information about system-level tasks, see [“View Ongoing and Completed System Tasks,”](#) on page 101.

The log can also include debug information, depending on your vCloud Director settings. See [“General System Settings,”](#) on page 90.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click the **My Cloud** tab and click **Logs** in the left pane.
- 4 Click the **Tasks** tab.
vCloud Director displays information about each organization-level task.
- 5 Double-click a task for more information.
Only system administrators can view the details about most tasks.

View System Events

View the system log to monitor system-level events. You can find and troubleshoot failed events and view events by user.

To view information about organization-level events, see [“View Organization Events,”](#) on page 102.

Procedure

- 1 Log in to the vCloud Director system as a system administrator.
- 2 Click the **Manage & Monitor** tab and click **Logs** in the left pane.
- 3 Click the **Events** tab.
vCloud Director displays information about each system-level event.
- 4 Double-click an event for more information.

View Organization Events

You can view the log for an organization to monitor organization-level events. You can find and troubleshoot failed events and view events by user.

To view information about system-level events, see [“View System Events,”](#) on page 102.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Organizations** in the left pane.
- 2 Right-click the organization name and select **Open**.
- 3 Click the **My Cloud** tab and click **Logs** in the left pane.
- 4 Click the **Events** tab.

vCloud Director displays information about each organization-level event.

- 5 (Optional) Double-click an event for more information.

Only system administrators can view the details about most events.

Monitor and Manage Blocking Tasks

You can monitor and manage tasks that are in a pending state as a result of blocking.

Although, you can monitor and manage blocking tasks using the vCloud Director Web console, it is generally expected that an external piece of code will listen for AMQP notifications and programmatically respond using the vCloud API.

Procedure

- 1 Click the **Manage & Monitor** tab and click **Blocking Tasks** in the left pane.
- 2 Right-click a task and select an action.

Option	Description
Resume	Resumes the task.
Abort	Aborts the task and deletes objects that were created as part of the task.
Fail	Fails the task but does not clean up objects that were created as part of the task. The status of the task and its objects is set to <i>Error</i> .

- 3 Type a reason and click **OK**.

View Usage Information for a Provider vDC

Provider vDCs supply compute, memory, and storage resources to organization vDCs. You can monitor provider vDC resources and add more resources if necessary.

Procedure

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

vCloud Director displays information about CPU, memory, and storage for each provider vDC.

View Usage Information for an Organization vDC

Organization vDCs supply compute, memory, and storage resources to organizations. You can monitor organization vDC resources and add more resources if necessary.

Procedure

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

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

Using vCloud Director's JMX Service

Each vCloud Director server host exposes a number of MBeans through JMX to allow for operational management of the server and to provide access to internal statistics.

Access the JMX Service by Using JConsole

You can use any JMX client to access the vCloud Director JMX service. JConsole is an example of a JMX client. For more information about the MBeans exposed by vCloud Director, see <http://kb.vmware.com/kb/1026065>.

Prerequisites

The host name of the vCloud Director host to which you connect must be resolvable by DNS using forward and reverse lookup of the fully-qualified domain name or the unqualified hostname.

Procedure

- 1 Start JConsole.
- 2 In the **Connection** menu, select **New Connection**.
- 3 Click **Remote Process** and type the JMX service URL.

The URL consists of the host name or IP address of the vCloud Director server, followed by the port number. For example, **example.com:8999**. The default port is 8999.

- 4 Type a vCloud Director system administrator user name and password and click **Connect**.
- 5 Click the **MBeans** tab.

Viewing the vCloud Director Logs

vCloud Director provides logging information for each cloud cell in the system. You can view the logs to monitor your cells and to troubleshoot issues.

You can find the logs for a cell at `/opt/vmware/cloud-director/logs`. [Table 10-1](#) lists the available logs.

Table 10-1. vCloud Director Logs

Log Name	Description
cell.log	Console output from the vCloud 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.

vCloud Director and Cost Reporting

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

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

You can specify the number of days of chargeback history that vCloud Director saves. See [“Modify General System Settings,”](#) on page 89.

Monitoring Quarantined Files

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

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

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

Quarantine Uploaded Files

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

Procedure

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

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

What to do next

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

View Quarantine Requests Using JConsole

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

Prerequisites

Upload quarantine is enabled.

Procedure

- 1 Start JConsole.
- 2 In the **Connection** menu, select **New Connection**.
- 3 Click **Remote Process** and type the JMX service URL.
The URL consists of the host name or IP address of the vCloud Director server, followed by the port number. For example, **example.com:8999**. The default port is 8999.
- 4 Type a vCloud Director system administrator user name and password and click **Connect**.
- 5 Click the **MBeans** tab and browse to the **org.apache.activemq > uuid > Queue > com.vmware.vcloud.queues.transfer.server.QuarantineRequest > Operations** node.
- 6 Select the `browseMessages()` operation.

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

- 6 Type a vCloud Director system administrator user name and password and click **Connect**.
- 7 Click the **MBeans** tab and browse to the **org.apache.activemq > uuid > Queue > com.vmware.vcloud.queues.transfer.server.QuarantineResponse > Operations** node.
- 8 Select the `sendTextMessage(string, string, string)` operation.
- 9 Paste the response message from your text editor in the first field and type a vCloud Director system administrator user name and password in the other fields.
- 10 Click **sendTextMessage**.

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

Roles and Rights

vCloud Director uses roles, and their associated rights, to determine which users and groups can perform which operations. System administrators can create and modify roles. System administrators and organization administrators can assign roles to users and groups in an organization.

vCloud Director includes several predefined roles.

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

Predefined Roles and Their Rights

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

[Table 11-1](#) lists the predefined vCloud 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/Reconfigure 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 a vApp	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: Access to VM Console	X	X	X	X	X	X
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	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/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: Edit Password Policy	X	X				
Organization vDC: View Organization vDCs	X	X				
User: View Group/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

A

- account lockout **98**
- activity log **101, 102**
- adding resources **15**
- adding vSphere resources **15**
- allocation models **29, 45**
- allocation pool allocation model **29, 45**
- AMQP broker **92**

B

- blocking tasks
 - about **92**
 - configuring settings **92**
 - configuring tasks **93**
- branding the UI
 - revert to system logo **97**
 - revert to system theme **97**

C

- catalog publishing, enabling **35**
- catalogs
 - adding **79**
 - creating **36**
 - publishing **35, 38**
- changing your password **14**
- Cisco Nexus 1000V **20**
- cloud cells
 - adding **68**
 - deleting **68**
 - maintenance message **68**
 - managing **67**
 - restarting **67**
 - starting **67**
 - stopping **67**
- cloud resources **17, 39**
- cost reporting **104**

D

- datastores
 - disk space warnings **42, 73**
 - enabling and disabling **41, 72**
 - monitoring capacity **42**
 - removing **73**
- DHCP network services **53**

E

- elastic vDC **29, 42, 45**
- email notifications **43, 85, 91**
- email settings **91**
- ESX/ESXi hosts
 - enabling and disabling **40, 71**
 - moving virtual machines **71**
 - preparing and unpreparing **40, 72**
 - repairing **41, 72**
 - upgrading agent **41, 72**
- extensions
 - aborting **103**
 - configuring AMQP **92**
 - failing **103**
 - resuming **103**
- external networks
 - adding **18**
 - adding IP addresses **49**
 - defined **18**
 - deleting **50**
 - name and description **49**
 - specification **49**

F

- fast provisioning **30, 46, 48, 82**
- firewall rules, setting the order **55**

G

- general system settings **89, 90**
- getting started **9**
- guest customization, preparing **12, 13**
- guided tasks **12**

I

- importing
 - media files **38**
 - vApp templates **37**

J

- JMX, accessing **104**
- JMX service **104**

K

- Kerberos realm **95**

L

LDAP

- configuring **93**
- customizing attributes **96**
- setting up the connection **94**
- support **93**
- synchronizing **96**
- testing the connection **95**
- LDAP groups, adding a description **86**
- leases, runtime and storage **23**
- licensing, vShield **17**
- linked clones **82**
- load balancer **97, 98**
- logging in **11**
- logs **104**
- Lost & Found **85**

M

- MBeans **104**
- media, uploading **37**
- Microsoft Sysprep **12, 13**
- monitoring, tasks and events **101**
- monitoring vCloud Director **101**
- MTU **21**

N

- NAT mapping rules, setting the order **57**
- network pools
 - adding Cloud isolated networks **66**
 - adding port groups **66**
 - adding VLAN IDs **67**
 - cloud network isolation-backed **20**
 - defined **19**
 - deleting **67**
 - name and description **66**
 - port group-backed **20**
 - setting the MTU **21**
 - VLAN-backed **19**
- network quota **31, 47**
- network services **53**
- Nexus 1000V **20**
- notifications, about **92**

O

organization networks

- adding **32**
- adding a firewall rule **54**
- adding a static route **61, 62**
- adding IP addresses **64**
- apply syslog server settings **65**
- configuring DHCP **53**
- configuring external IPs **56**
- configuring firewalls **54**

- configuring IP translation **57**
- configuring NAT **56, 57**
- configuring port forwarding **56**
- configuring services **53**
- connected vApp templates **64**
- connected vApps **64**
- create VPN tunnel **58–60**
- creating **50**
- deleting **64**
- enabling site-to-site VPN **58**
- enabling static routing **60**
- external direct **32, 51**
- external NAT-routed **33, 51**
- internal **34, 52**
- IP masquerade **55**
- managing **50**
- modifying DNS **65**
- modifying the name and description **65**
- ordering firewall rules **55**
- ordering NAT mapping rules **57**
- resetting **63**
- view syslog server settings **65**
- viewing IP usage **64**
- organization vDCs
 - allocating storage **30, 46**
 - allocation model settings **48**
 - allocation models **29, 45**
 - changing description **48**
 - changing name **48**
 - confirm settings **31, 47**
 - creating **28, 43, 44**
 - deleting **47**
 - enabling or disabling **47**
 - monitoring usage **103**
 - naming **31, 47**
 - network pools **49**
 - network quota **31, 47**
 - selecting a network pool **31, 47**
 - selecting a provider vDC **29, 44**
 - selecting the organization **44**
 - storage capacity **48**
- organizations
 - adding local users **26**
 - allocating resources **28**
 - catalog publishing **77**
 - confirm settings **27**
 - creating **24**
 - deleting **75**
 - email preferences **26, 78**
 - enabling or disabling **75**
 - full name and description **76**
 - LDAP options **25, 76**

- lease settings **27, 78**
 - limit settings **27, 78**
 - managing **75**
 - managing resources **79**
 - monitoring events **102**
 - monitoring tasks **102**
 - naming **25**
 - publishing catalogs **26**
 - quota settings **27, 78**
 - renaming **76**
 - SMTP server **26**
 - SMTP settings **78**
 - users and groups **80**
 - vApps **80**
 - OVF upload **36**
- P**
- password policy **98**
 - pay-as-you-go allocation model **29, 45**
 - provider vDCs
 - adding resource pools **42**
 - adding storage capacity **41**
 - changing name **40**
 - creating **17**
 - defined **17**
 - deleting **39**
 - enabling or disabling **39**
 - managing **39**
 - monitoring usage **103**
 - publishing catalogs **35, 38**
- Q**
- quarantine service
 - accepting requests **106**
 - enabling **105**
 - overview **105**
 - rejecting requests **106**
 - viewing requests **105**
 - quick start tasks **12**
- R**
- reservation pool allocation model **29, 45**
 - roles
 - copying **87**
 - creating **86**
 - deleting **87**
 - editing **87**
 - roles and rights **107**
 - runtime leases **23**
- S**
- shadow virtual machines **82**
 - SMTP server **78**
 - SMTP settings **91**
 - storage leases **23**
 - stranded items
 - deleting **73**
 - force deleting **74**
 - system
 - monitoring tasks **101**
 - roles and rights **86**
 - system administrators
 - creating accounts **83**
 - deleting **84**
 - disabling **84**
 - editing accounts **84**
 - from LDAP **84**
 - LDAP groups **85, 86**
 - system events **102**
 - system notification settings **91**
 - system settings **89**
- T**
- Technical Support, to obtain **7**
 - thin provisioning **30, 46, 48**
- U**
- upgrade vCenter Server **70**
 - uploading
 - media **37**
 - vApps **36**
 - user preferences **14**
- V**
- vApps
 - adding vSphere virtual machines **80**
 - backing up **81**
 - force stopping **81**
 - importing from vSphere **80**
 - placing in maintenance mode **81**
 - VCD public console proxy address **98**
 - VCD public REST API base URL **98**
 - VCD public URL **97**
 - vCenter Chargeback **104**
 - vCenter Server, upgrade **70**
 - vCenter Servers
 - assigning a vShield license **17**
 - attaching **15, 16**
 - confirming settings **16**
 - connecting **16**
 - connection settings **69**
 - disabling **70**
 - reconnecting **70**
 - removing **70**
 - vShield Manager settings **71**

- vCloud Director overview **9**
- virtual machines, importing from vSphere **80**
- VPN **58**
- vShield, licensing **17**
- vShield for VMware Cloud Director license **17**
- vShield Manager
 - connecting **16**
 - settings **71**
- vSphere
 - datastores **72**
 - importing media files from **38**
 - importing virtual machines from **37**
 - resources **69**
 - stranded items **73**
- vSphere distributed switches, setting the MTU **21**

W

- Web console, logging in **11**