vCloud Director User's Guide

vCloud Director 8.20

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

Contents

vCloud Director User's Guide

The *VMware vCloud Director User's Guide* provides information about managing organizations, catalogs, vApps, and virtual machines.

Intended Audience

This book is intended for anyone who wants to set up and configure organizations in VMware vCloud Director. The information in this book is written for non-system administrators, including organization administrators who will create and set up vApps, catalogs, and virtual machines.

Getting Started with vCloud Director 1

When you log in to the vCloud Director Web console, the **Home** tab provides access to your resources and links to common tasks.

You can also set your user preferences and view the product help.

This chapter includes the following topics:

■ "Understanding VMware vCloud Director," on page 9

■ "Log In to the Web Console," on page 10

■ "Using vCloud Director," on page 10

■ "Set User Preferences," on page 11

■ "Change Your Password," on page 11

Understanding VMware vCloud Director

VMware® vCloud Director provides role-based access to a Web console that allows the members of an organization to interact with the organization's resources to create and work with vApps and virtual machines.

Before you can access your organization, a vCloud Director system administrator must create the organization, assign it resources, and provide the URL to access the Web console. Each organization includes one or more organization administrators, who finishes setting up the organization by adding members and setting policies and preferences. After the organization is set up, non-administrator users can log in to create, use, and manage virtual machines and vApps.

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.

Users and Groups

An organization can contain an arbitrary number of users and groups. Users can be created locally 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.

Virtual Datacenters

An organization virtual datacenter provides resources to an organization. Virtual datacenters provide an environment where virtual systems can be stored, deployed, and operated. They also provide storage for virtual CD and DVD media. An organization can have multiple virtual datacenters.

Organization Virtual Datacenter Networks

An organization virtual datacenter network is contained within a vCloud Director organization virtual datacenter and is available to all the vApps in the organization. An organization virtual datacenter network allows vApps within an organization to communicate with each other. An organization virtual datacenter network can be connected to an external network or isolated and internal to the organization. Only system administrators can create organization virtual datacenter networks, but organization administrators can manage organization virtual datacenter networks, including the network services they provide.

vApp Networks

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

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. Organizations administrators can copy items from public catalogs to their organization catalog.

Log In to the Web Console

Use the organization URL to log in to your organization and access the Web console.

Contact your organization administrator if you do not know the organization URL. See the *vCloud Director Release Notes* for information about supported browsers and configurations.

Procedure

1   In a browser, type the URL of your organization and press Enter.

For example, type `https://vcloud.example.com/cloud/org/myOrg`.

2   Type your user name and password and click **Login**.

What to do next

The Web console displays a list of the common tasks and resources available to you based on your role. An organization administrator can click the **Set up this organization** link on the **Home** tab to finish setting up a newly created organization. See "Set Up an Organization," on page 28 for more information.

Using vCloud Director

When you log into vCloud Director, the first page you see is the Home page. The information that appears on this page are the most common tasks for your role.

Organization administrators see the **Set up this organization** link as their first task. They also see tasks under these headings.

■   **Organizations and resources**

- **Content**

- **Users & Groups**

The vApps in your organization are displayed for easy access.

Catalog authors see links to these tasks.

- **Add Cloud Computer System**

- **Build new vApp**

- **Manage Catalogs**

- **New Catalog**

vApp authors see links to these tasks.

- **Add Cloud Computer System**

- **Build new vApp**

vApp users see links to these tasks.

- **Add Cloud Computer System**

The vApps in your organization are displayed for easy access.

Console Access Only users have a read-only access to vCloud Director.

Set User Preferences

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

Procedure

1 In the title bar of the Web console, click **Preferences**.

2 Click the **Defaults** tab.

3 Select the page to display when you log in.

4 Select the number of days or hours before a runtime lease expires that you want to receive an email notification.

5 Select the number of days or hours before a storage lease expires that you want to receive an email notification.

6 Click the **Change Password** tab.

7 (Optional) Type your current password and type your new password twice.

8 Click **OK**.

Change Your Password

If you have a local user account, you can change your password.

Procedure

1 Log in to your organization.

2 In the title bar of the Web console, click **Preferences**.

3 On the **Change Password** tab, type your current password, type your new password, and retype your new password.

4   Click **OK**.

vCloud Director logs you out.

What to do next

Log in using your new password.

Managing Cloud Resources

<div style="text-align: right; font-size: 3em; font-weight: bold; color: gray;">2</div>

A vCloud Director system administrator creates and assigns virtual datacenters and networks to an organization. An organization administrator can view information about these resources and perform a limited set of management tasks. Contact your system administrator if you need more organization virtual datacenters or organization virtual datacenter networks..

This chapter includes the following topics:

- "Managing Virtual Datacenters," on page 13
- "Managing Organization Virtual Datacenter Networks," on page 14
- "Managing Expired Items," on page 25

Managing Virtual Datacenters

The system administrator creates virtual datacenters to provide your organization with provide CPU, memory, storage, and networking resources. An organization administrator can view virtual datacenter properties and manage the vApps, vApp templates, and media items they contain.

Display Virtual Datacenter Contents and Properties

Open a virtual datacenter to view and manage the vApps, vApp templates, and media object it contains, to send administrative notifications to its users, and to view its other properties.

Prerequisites

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

Procedure

1   Click **Administration**.

2   In the left pane, select **Cloud Resources > Virtual Datacenters**.

   A list of virtual datacenters in your organization appears in the right pane.

   - To view virtual datacenter contents, right-click a virtual datacenter in the list and select **Open**. The vApps, vApp templates, media, and networks contained by this virtual datacenter are displayed. When you click through each tab, you can right click on an object to see the operations you can complete.

   - To manage the distributed firewall for a virtual datacenter, right-click it and select **Manage Firewall** to open the Distributed Firewall page of the vCloud Director Tenant Portal.

■ To send an administrative notification to all users of the virtual datacenter, select **Notify Users**. Fill in the Notify Users form with a subject and message, then click **Send Email** to email the notification to all users who own vApps, vApp templates, or media items in the virtual datacenter.

Review Virtual Datacenter Properties

You can review the properties of the virtual datacenters that are assigned to your organization.

Prerequisites

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

Procedure

1 Click **Administration**.

2 Select **Cloud Resources > Virtual Datacenters**.

3 Select a virtual datacenter, right-click, and select **Properties**.

4 Review the properties and click **OK**.

What to do next

To modify your organizational virtual datacenters, contact your system administrator.

Monitor Virtual Datacenter Resource Use

You can monitor resource consumption in virtual datacenters assigned to your organization and determine when to request additional resources.

Prerequisites

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

Procedure

1 Click **Administration**.

2 Select **Cloud Resources > Virtual Datacenters**.

3 Click the **Monitor** button.

Details about the processor, memory, storage, and allocation model appear.

What to do next

Contact your system administrator if you need more capacity.

Managing Organization Virtual Datacenter Networks

Organization virtual datacenter networks are created and assigned to your organization virtual datacenter by a system administrator. An organization administrator can view information about networks, configure network services, and more.

You can use direct, routed, or internal organization virtual datacenter networks.

Table 2-1. Types of Organization Virtual Datacenter Networks

Organization Virtual Datacenter Network Type	Description
Direct	Accessible by multiple organizations. Virtual machines belonging to different organizations can connect to and see traffic on this network.
	This network provides direct layer 2 connectivity to virtual machines outside of the organization. Virtual machines outside of this organization can connect to virtual machines in the organization directly.
Routed	Accessible only by this organization. Only virtual machines in this organization can connect to this network.
	This network also provides controlled access to an external network. System administrators and organization administrators can configure network address translation (NAT), firewall, and VPN settings to make specific virtual machines accessible from the external network.
Internal	Accessible only by this organization. Only virtual machines in this organization can connect to and see traffic on this network.
	This network provides an organization with an isolated, private network that multiple vApps can connect to. This network provides no connectivity to machines outside this organization. Machines outside of this organization have no connectivity to machines in the organization.

Configuring Oganization Virtual Datacenter Network Services

An organization administrator can configure services, such as DHCP, firewalls, network address translation (NAT), VPN, and static routing for certain organization virtual datacenter networks.

The network services available depend on the type of organization virtual datacenter network.

Table 2-2. Network Services Available by Network Type

Organization Virtual Datacenter Network Type	DHCP	Firewall	NAT	VPN	Static Routing
Direct					
Routed	X	X	X	X	X
Internal	X				

Configure DHCP for an Organization VDC Network

Organization administrators can configure routed and isolated organization virtual datacenter networks to provide DHCP services.

The DHCP service of an organization VDC network provides IP addresses from its address pool to VM NICs that are configured to request an address from DHCP. The service provides the address when the VM is powered on.

Prerequisites

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

■　Verify that you have a routed organization virtual datacenter network or an internal organization virtual datacenter network.

Procedure

1　Click **Administration**.

2　In the left pane, select **Cloud Resources > Virtual Datacenters**.

　　A list of virtual datacenters in your organization appears in the right pane.

3　Right-click a virtual datacenter in the list and select **Open**.

4　Click the **Org VDC Networks** tab, right-click a network name and select **Configure Services**.

5　Select **Enable DHCP** on the DHCP tab.

　　Addresses requested by DHCP clients are taken from the DHCP pool shown on this tab. You can edit this pool or create new ones.

6　(Optional) Create or modify DHCP pools for this network.

- To edit an existing DHCP pool, select it and click **Edit**.

- To create a new DHCP pool, click **Add**.

　　Specify an IP address range for the pool. This address range cannot overlap with the static IP pool for the organization VDC. Every DHCP address pool is created with system-defined values for **Default lease time** and **Max lease time**. You can override these defaults if you need to.

7　Click **OK** to save your changes.

Configure the Firewall for an Organization Virtual Datacenter Network

An organization administrator can configure certain organization virtual datacenter networks to provide firewall services. Enable the firewall on an organization virtual datacenter network to enforce firewall rules on incoming traffic, outgoing traffic, or both.

When you enable the firewall, you can specify a default firewall action to deny all incoming and outgoing traffic or to allow all incoming and outgoing traffic. You can also add specific firewall rules to allow or deny traffic that matches the rules to pass through the firewall. These rules take precedence over the default firewall action. See "Add a Firewall Rule to an Organization Virtual Datacenter Network," on page 17.

Prerequisites

Verify that a routed organization virtual datacenter network is in place.

Procedure

1　Click **Administration** and select the organization virtual datacenter.

2　Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name, and select **Configure Services**.

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

4　Select the default firewall action.

Option	Description
Deny	Blocks all traffic except when overridden by a firewall rule.
Allow	Allows all traffic except when overridden by a firewall rule.

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

6　Click **OK**.

Add a Firewall Rule to an Organization Virtual Datacenter Network

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

When you add a new firewall rule to an organization virtual datacenter network, it appears at the bottom of the firewall rule list. For information about how to set the order in which firewall rules are enforced, see "Reorder Firewall Rules for an Organization Virtual Datacenter Network," on page 18.

Prerequisites

Verify that you have a routed organization virtual datacenter network and enable the firewall for the organization virtual datacenter network. See "Configure the Firewall for an Organization Virtual Datacenter Network," on page 16

Procedure

1   Click **Administration** and select the organization virtual datacenter.

2   On the **Org VDC Networks** tab, right-click the organization virtual datacenter network name and select **Configure Services**.

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

4   Type a name for the rule.

5   Type the traffic **Source**.

Option	Description
IP address	Type a source IP address to apply this rule on.
Range of IP addresses	Type a range of source IP addresses to apply this rule on.
CIDR	Type the CIDR notation of traffic to apply this rule on.
`internal`	Apply this rule to all internal traffic.
`external`	Apply this rule to all external traffic.
`any`	Apply this rule to traffic from any source.

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

7   Type the traffic **Destination**.

Option	Description
`IP address`	Type a destination IP address to apply this rule on.
`Range of IP addresses`	Type a range of destination IP addresses to apply this rule on.
`CIDR`	Type the CIDR notation of traffic to apply this rule on.
internal	Apply this rule to all internal traffic.
external	Apply this rule to all external traffic.
any	Apply this rule to traffic with any destination.

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

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

10 Select the action.

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

11 Select the **Enabled** check box.

12 (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.

13 Click **OK** and click **OK** again.

Reorder Firewall Rules for an Organization Virtual Datacenter Network

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

When you add a firewall rule to an organization virtual datacenter network, the new rule appears at the bottom of the firewall rule list. To enforce the new rule before an existing rule, reorder the rules.

Prerequisites

Verify that a routed organization virtual datacenter network with two or more firewall rules is in place.

Procedure

1 Click **Administration** and select the organization virtual datacenter.

2 Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name, and select **Configure Services**.

3 Click the **Firewall** tab.

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

5 Click **OK**.

Enable VPN for an Organization Virtual Datacenter Network

An organization administrator can enable VPN for an organization virtual datacenter network, then create a secure tunnel to another network.

vCloud Director supports VPN between organization virtual datacenter networks in the same organization and remote networks.

Prerequisites

Verify that you have a routed organization virtual datacenter network.

Procedure

1 Click **Administration** and select the organization virtual datacenter.

2 Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name, and select **Configure Services**.

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

4 (Optional) Click **Configure Public IPs**, type a public IP address, and click **OK**.

5 Click **OK**.

What to do next

Create a VPN tunnel to another network.

Create a VPN Tunnel In an Organization

An organization administrator can create a VPN tunnel between two organization virtual datacenter networks in the same organization.

If the tunnel endpoints have a firewall between them, configure the firewall to allow the following IP protocols and UDP ports:

- IP Protocol ID 50 (ESP)

- IP Protocol ID 51 (AH)

- UDP Port 500 (IKE)

- UDP Port 4500

Prerequisites

Verify that you have at least two routed organization virtual datacenter networks with nonoverlapping IP subnets and VPN enabled on both networks.

Procedure

1   Click **Administration** and select the organization virtual datacenter.

2   Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name, and select **Configure Services**.

3   Click the **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

An organization administrator can create a VPN tunnel between two organization virtual datacenter networks in different organizations. The organizations can be part of the same vCloud Director installation or a different installation.

Prerequisites

Verify that you have a routed organization virtual datacenter network in each of the organizations. The organization virtual datacenter networks must have IP subnets that do not overlap and a site-to-site VPN enabled.

If the tunnel endpoints have a firewall between them, 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

Procedure

1   Click **Administration** and select the organization virtual datacenter.

2   Click the **Org VDC Networks** tab, right-click the organization virtual datacenter network name, and select **Configure Services**.

3   Click the **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	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	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	User name of an organization administrator or system administrator that has access to the organization.
Password	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

An organization administrator can create a VPN tunnel between an organization virtual datacenter network and a remote network.

If the tunnel endpoints have a firewall between them, 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

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

Verify that you have a routed organization virtual datacenter network and a routed remote network that uses IPSec.

Procedure

1   Click **Administration** and select the organization virtual datacenter.

2   Select **Cloud Resources > Networks**.

3   Click the **Organization VDC Network** tab, right-click the organization virtual datacenter network name, and select **Configure Services**.

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

5   Type a name and optional description.

6   Select **a remote network** from the drop-down menu.

7   Type the peer settings.

See VMware Knowledge Base article https://kb.vmware.com/kb/2051370.

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

vCloud Director configures the organization peer network endpoint.

What to do next

Manually configure the remote peer network endpoint.

Enable Static Routing for an Organization Virtual Datacenter Network

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

Prerequisites

Verify that a routed organization virtual datacenter network is in place.

Procedure

1   Click **Administration**.

2   Select **Cloud Resources > Networks**.

3   Right-click the organization virtual datacenter network name and select **Configure Services**.

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

What to do next

Create static routes.

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

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

You cannot add static routes between overlapping networks or fenced vApps. After you add a static route to an organization virtual datacenter network, configure the network firewall rules to allow traffic on the static route. 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 you change the parent network of a vApp, delete a vApp, or delete a vApp network, and the vApp includes static routes, those routes cannot function and you must remove them manually.

Prerequisites

Verify that the following conditions are met.

■   A routed organization virtual datacenter network is in place.

■   Static routing is enabled on the organization virtual datacenter network.

■   Two vApp networks are routed to the organization virtual datacenter network.

■   The vApp networks are in vApps that were started at least once.

Procedure

1   Click **Administration**.

2   Select **Cloud Resources > Networks**.

3   Right-click the organization virtual datacenter network name and select **Configure Services**.

4   Click the **Static Routing** tab and click **Add**.

5   Type a name, network address, and next hop IP address.

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

6   Select **Within this network**, and click **OK**.

7   Click **OK**.

8   Repeat Step 4 through Step 7 to add a route to the second vApp network.

Example: Static Routing Example

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

Table 2-3. 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 2-4. 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	In this network
vApp Network 2	tovapp2	192.168.2.0/24	192.168.0.101	In this network

What to do next

Create firewall rules to allow traffic on the static routes.

Add Static Routes Between vApp Networks Routed to Different Organization Virtual Datacenter Networks

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

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

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

Prerequisites

Verify that you have the following items.

■ Two organization virtual datacenter networks routed to the same external network.

■ Static routing is enabled on both organization virtual datacenter networks.

■ A vApp network is routed to each organization virtual datacenter network.

■ The vApp networks are in vApps that were started at least once.

Procedure

1   Click **Administration** and select the organization virtual datacenter.

2   Click the Org virtual datacenter Networks tab, right-click the organization virtual datacenter network name, and select **Configure Services**.

3   Click the **Static Routing** tab and 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 virtual datacenter 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 virtual datacenter 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 Step 2 through Step 8 to add static routes to the second organization virtual datacenter network.

Example: Static Routing Example

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

Table 2-5. 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 VDC Network 1	192.168.0.0/24	10.112.205.101
Org VDC Network 2	192.168.10.0/24	10.112.205.100

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

Table 2-6. Static Routing Settings for Org VDC 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 2-7. Static Routing Settings for Org VDC 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.

Reset an Organization Virtual Datacenter Network

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

No network services are available while an organization virtual datacenter network resets.

Prerequisites

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

■ Verify that you have an external NAT-routed organization virtual datacenter network or an internal organization network.

■ Verify that you have organization administrator privileges.

Procedure

1   Click **Administration** and select the organization virtual datacenter.

2   Right-click an organization virtual datacenter network, and select **Reset Network**.

3   Click **Yes**.

View IP Use for an Organization Virtual Datacenter Network

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

Prerequisites

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

Procedure

1   Click **Administration** and select the organization virtual datacenter.

2   Right-click an organization virtual datacenter network, and select **IP Allocations**.

Add IP Addresses to an Organization Virtual Datacenter Network IP Pool

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

You cannot add IP addresses to external organization virtual datacenter networks that have a direct connection.

Prerequisites

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

Procedure

1 Click **Administration** and select the organization virtual datacenter.

2 Right-click an organization virtual datacenter network 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**.

View vApps and vApp Templates That Use an Organization Virtual Datacenter Network

You can view a list of the all the vApps and vApp templates that include virtual machines with a NIC connected to an organization virtual datacenter network.

Prerequisites

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

Procedure

1 Click **Administration** and select the organization virtual datacenter.

2 Right-click an organization virtual datacenter network and select **Connected vApps**.

3 Click **OK**.

Managing Expired Items

When vApps or vApp templates expire, you can determine whether you want to renew or delete them.

Manage Expired vApps

You can display a list of expired vApps, delete them, or restore them to your organization.

The organization policy for what to do when a vApp storage lease expires is set to **Move to Expired Items**. See "Configure Organization Lease, Quota, and Limit Settings," on page 30.

Prerequisites

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

Procedure

1 Select **My Cloud > Expired Items**.

2   On the **Expired vApps** tab, review the list of expired vApps.

3   Right-click a vApp and select **Delete** or **Renew** and click **Yes**.

If you selected **Delete**, the vApp is deleted from the list. If you selected **Renew**, the restored vApp appears on the **vApps** page.

Manage Expired vApp Templates

You can display a list of expired vApp templates and delete them or restore them to your organization.

The organization policy for what to do when a vApp template storage lease expires is set to **Move to Expired Items**. See "Configure Organization Lease, Quota, and Limit Settings," on page 30.

Prerequisites

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

Procedure

1   Select **My Cloud > Expired Items**.

2   Click the **Expired vApp Templates** tab.

3   Right-click on a vApp template, select **Delete** or **Renew**, and click **Yes**.

If you selected **Delete**, the vApp template is deleted from the list. If you selected **Renew**, the vApp template is restored to its catalog.

Working in an Organization 3

Most operations in vCloud Director occur in an organization. The system administrator creates the organization and assigns an organization administrator to it.

The system administrator emails the URL of the organization to the organization administrator, who can log in to the organization and set it up. In the Home page the organization administrator clicks the **Set up the Organization** link to assign resources and manage a variety of operations on the organization.

This chapter includes the following topics:

■ "Understanding Leases," on page 27

■ "Set Up an Organization," on page 28

■ "Review Your Organization Profile," on page 31

■ "Modify Your Email Settings," on page 31

■ "Modify Your Organization's Policies," on page 32

■ "Set Default Windows Domain for Virtual Machines in This Organization," on page 33

■ "Enable Your Organization to Use a SAML Identity Provider," on page 33

■ "Manage Users and Groups in Your Organization," on page 35

■ "Manage Resources in Your Organization," on page 35

■ "Manage Virtual Machines in Your Organization," on page 35

■ "Viewing Organization Log Tasks and Events," on page 36

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 30.

Users can configure email notification to receive a message before a runtime or storage lease expires. See "Set User Preferences," on page 11 for information about lease expiration preferences.

Set Up an Organization

After you receive the URL of your organization from the system administrator, you must set it up. On the vCloud Director **Home** page, click **Set up this organization**.

Prerequisites

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

Procedure

1   Change the Organization Full Name on page 28

    You can change the full name of an organization. This name appears in the Cloud Director application header when users log in.

2   Import Users and Groups on page 29

    You can add users and groups from an LDAP or SAML server to the organization and assign them a role within the organization.

3   Add Local Users to the Organization on page 29

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

4   Configure Email Preferences on page 29

    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.

5   Configure Organization Lease, Quota, and Limit Settings on page 30

    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.

Change the Organization Full Name

You can change the full name of an organization. This name appears in the Cloud Director application header when users log in.

Prerequisites

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

Procedure

1   On **Name this Organization** page, in the **Organization full name**, type the new full name.

2   (Optional) Type a description of the organization.

3   Click **Next.**

Import Users and Groups

You can add users and groups from an LDAP or SAML server to the organization and assign them a role within the organization.

Prerequisites

Verify that your organization has a valid connection to an LDAP or SAML server.

Procedure

1   Click **Import**.

2   Select the type of server to import from.

3   Type a full or partial name of a user or group and click **Search**.

If you are importing from a SAML server, you must include the domain name (ex. `user@domain.com`).

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

5   Select a role for the users and groups and click **OK**.

6   Click **Next**.

Add Local Users to the Organization

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

Procedure

1   Click **Add**.

2   Type a user name and password.

3   Assign a role to the user.

4   (Optional) Type the contact information for the user.

5   Select **Unlimited** or type a user quota for stored and running virtual machines and click **OK**.

These quotas limit the user's ability to consume storage and compute resources in the organization. If you set a quota here that is different from the quota set at the organization level, this quota takes precedence.

6   Click **Next**.

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 27.

Procedure

1   Select the lease options for vApps and vApp templates.

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

2   Select the quotas for running and stored virtual machines.

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

3   Select the limits for resource intensive operations.

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

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

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

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

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

6   Click **Next**.

Review Your Organization Profile

You can review and modify some of the information in your organization's profile

Prerequisites

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

Procedure

1   Click **Administration**.

2   In the left pane, select **Settings > General**.

3   You can complete these operations.

   ■   Review your organization's default URL.

   ■   Modify your organization's full name.

   ■   Type a description.

4   Click **Apply**.

Modify Your Email Settings

You can review and modify the default email settings that were set when the system administrator created your organization.

vCloud Director sends alert emails when it has important information to report, such as when a datastore is running out of space. By default, an organization sends email alerts to the system administrators or list of email addresses specified at the system level using an SMTP server specified at the system level. You can modify the email settings at the organization level if you want vCloud Director to send alerts for that organization to a different set of email addresses than those specified at the system level or you want the organization to use a different SMTP server to send alerts than the server specified at the system level.

Prerequisites

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

Procedure

1   Click **Administration**.

2   In the left pane, select **Settings > Email**.

3   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.

4   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.

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

6   Click **Apply**.

Modify Your Organization's Policies

You can review and modify the default policies that were set by the system administrator when your organization was created.

Prerequisites

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

Procedure

1   Click **Administration**.

2   In the left pane, select **Settings > Policies**.

3   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.

4   Select the quotas for running and stored virtual machines.

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

5   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.

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

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

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

7   (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.

8   Click **Apply**.

Set Default Windows Domain for Virtual Machines in This Organization

You can set a default Windows domain which virtual machines created in your organization can join. Virtual machines can always join a domain for which they have credentials, regardless of whether or not you specify a default domain.

Prerequisites

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

Procedure

1   Click **Administration**.

2   In the left pane, select **Settings > Guest Personalization**.

3   Select the **Enable domain join for virtual machines in this organization**.

4   Type the domain name, domain user name, domain password.

    These credentials apply to a regular domain user, not a domain administrator.

5   Click **Apply**.

Enable Your Organization to Use a SAML Identity Provider

Enable your organization to use a SAML identity provider, also called single sign-on, to import users and groups from a SAML identity provider and allow imported users to sign on to the organization with the credentials established in the SAML identity provider.

Prerequisites

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

■   Verify that you have access to an OpenAM or Active Directory Federation Services SAML identity provider.

■   Verify that your system has updated JCE unlimited strength jurisdiction policy files. See "Install Java Cryptography Extension Unlimited Strength Jurisdiction Policy Files" in the *vCloud Director Administrator's Guide*.

■   Create an XML file with the following metadata from your SAML identity provider.

    ■   The location of the single sign-on service

    ■   The location of the single logout service

    ■   The location of the service's X.509 certificate

    For information on configuring and acquiring metadata from an OpenAM or Active Directory Federation Services SAML provider, consult the documentation for your SAML provider.

■   The system will extract these attributes from the SAML token (if available) and use them for interpreting the corresponding pieces of information about the user attempting to log in.

    ■   `email address = "EmailAddress"`

    ■   `user name = "UserName"`

    ■   `full name = "FullName"`

- **`user's groups = "Groups"`**

- **`user's roles = "Roles"`** (this attribute is configurable)

Group information is necessary if the user is not directly imported but is expected to be able to log in by virtue of membership in imported group(s). A user may belong to multiple groups and hence can have multiple roles during a session.

If an imported user or group is assigned the Defer to Identity Provider role, the roles are assigned based on the information gathered from the Roles attribute in the token. If a different attribute is used, this attribute name can be configured via API only and only the Roles attribute is configurable. If the Defer to Identity Provider role is used, but no role information can be extracted, the user can log in but not have any rights to perform any activities.

Procedure

1   Click **Administration**.

2   In the left pane, select **Settings > Federation**.

3   Enter an **Entity Id** for the Service Provider.

The Entity Id uniquely identifies your organization to your Identity Provider. Previously, the system generated an Entity Id for you. To ensure backward compatibility and continued functionality, the system will continue to use this generated value, but it is strongly recommended that organization(s) use their own Entity Id specific to their identity provider.

Once an Entity Id is set, it cannot be deleted, but can be changed. Any changes to the Entity Id will require a full SAML reconfiguration in order for it to continue functioning correctly. For more information on Entity Ids, see Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) 2.0.

4   Review the Certificate Expiration date and If necessary, click **Regenerate** to regenerate the certificate used to sign federation messages.

The certificate is included in the SP (vCloud Director) metadata. This certificate is used for both encryption and signing. Either or both of these may be required depending on how trust is established between SP and IDP and parameters that are agreed upon as a part of this trust establishment.

5   Click the **Metadata** link to download the Service Provider metadata.

This must be provided to your IDP as a part of trust establishment between your organization and your IDP. You can review the document to understand the SP parameters included as part of this process, but do not edit this document as it will interfere with correct SAML behavior.

6   Select **Use SAML Identity Provider**.

7   Copy and paste the IDP SAML provider metadata XML into the text box or click **Browse** to upload the metadata XML file.

8   Click **Apply**.

What to do next

- Configure your SAML provider with vCloud Director metadata. See your SAML provider's documentation and the *vCloud Director Installation and Upgrade Guide*.

- Import users and groups from your SAML provider.

Manage Users and Groups in Your Organization

You can manage the roles and rights that users and groups have in your organization.

Prerequisites

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

Procedure

1　Click **Administration**.

2　In the left pane, select **Members > Users** or **Members > Groups**.

　You can modify properties or roles.

3　Right-click the user or group and select **Properties**.

4　Make the necessary changes and click **OK**.

Your user or group settings are updated.

Manage Resources in Your Organization

You must monitor and manage the resources you add to your organization.

Prerequisites

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

Procedure

1　Click **Administration**.

2　In the left pane, under **Cloud Resources**, select **Virtual Datacenters**.

The virtual datacenters in your organization appear in the right pane. See also Chapter 2, "Managing Cloud Resources," on page 13

Manage Virtual Machines in Your Organization

You can manage virtual machines in your organization. Virtual machines provide access to vCloud Director operations at the virtual machine console level.

Prerequisites

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

Procedure

1　Click **My Cloud**.

2　In the left pane, select **VMs**.

3　Select a virtual machine, right-click, and select **Properties**.

4　Modify the relevant properties in each of the tabs and click **OK**.

What to do next

For more information on managing virtual machines, see Chapter 8, "Working with Virtual Machines," on page 85.

Viewing Organization Log Tasks and Events

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

vCloud Director tasks are 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 are one-time occurrence that indicate an important part of an operation or a significant state change for a vCloud Director object. vCloud Director also logs an event every time a user logs in, and notes whether the attempt was successful or not.

View Organization Events

You can view the log for an organization to monitor organization-level events. Failed events and view events are listed by user.

Prerequisites

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

Procedure

1 Click the **My Cloud**.

2 In the left pane, click **Logs**.

3 Click the **Events** tab.

   vCloud Director displays information about each organization-level event.

4 Double-click an event for more information.

   Only system administrators can view the details about most events.

View Organization Tasks

You can view the tasks in an organization, which helps you monitor and troubleshoot more effectively.

Prerequisites

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

Procedure

1 Click **My Cloud**.

2 In the left pane, click **Logs**.

3 On the **Tasks** tab, you can examine the tasks in the organization.

4 Select a task, right-click, and select **Open**.

5 Review the information and click **OK**.

What to do next

To troubleshoot a failed task, contact your system administrator.

Working with Catalogs

4

A catalog is a container for vApp templates and media files in an organization. Organization administrators and catalog authors can create catalogs in an organization. Catalog contents can be shared with other users or organizations in the vCloud Director installation or published externally for access by organizations outside the vCloud Director installation.

vCloud Director contains private catalogs, shared catalogs, and externally accessible catalogs. Private catalogs include vApp templates and media files that you can share with other users in the organization. If a system administrator enables catalog sharing for your organization, you can share an organization catalog to create a catalog accessible to other organizations in the vCloud Director installation. If a system administrator enables external catalog publishing for your organization, you can publish an organization catalog for access by organizations outside the vCloud Director installation. An organization outside the vCloud Director installation must subscribe to an externally published catalog to access its contents.

You can upload an OVF package directly to a catalog, save a vApp as a vApp template, or import a vApp template from vSphere. See "Upload an OVF Package as a vApp Template," on page 49 and "Save a vApp as a vApp Template," on page 52. You can upload media files directly to a catalog. See "Upload Media Files," on page 43

Members of an organization can access vApp templates and media files that they own or that are shared with them. Organization administrators and system administrators can share a catalog with everyone in an organization or with specific users and groups in an organization. See "Share A Catalog," on page 39.

This chapter includes the following topics:

- "Add a New Catalog," on page 37
- "Access a Catalog," on page 39
- "Share A Catalog," on page 39
- "Change the Owner of a Catalog," on page 40
- "Delete a Catalog," on page 40
- "Change the Properties of a Catalog," on page 41
- "Subscribe to an External Catalog Feed," on page 41

Add a New Catalog

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

Prerequisites

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

Procedure

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

2 On the **Catalogs** tab, click **Add Catalog**.

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

4 Select the type of storage to use for vApp templates and ISOs in this catalog and click **Next**.

Option	Description
Use any available storage in the organization	This catalog uses any available storage in the organization.
Pre-provision storage on specific storage policy	Select a virtual datacenter storage policy to use for this catalog's vApp templates and ISOs and click **Add**. The selected storage policy causes the vApp template size to count against your catalog storage quota.

5 Click **Add Members**.

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

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

■ Select **Everyone in this organization** to grant catalog access to all users and groups in the organization.

■ Select **Specific users and groups** to grant catalog access to certain users or groups and click **Add**.

b Select the access level for users with access to this catalog from the drop-down menu and click **OK**.

■ Select **Read Only** to grant read access to the catalog's vApp templates and ISOs.

■ Select **Read/Write** to grant read access to the catalog's vApp templates and ISOs, and to allow user to add vApp templates and ISOs to the catalog.

■ Select **Full Control** to grant full access to the catalog's contents and settings.

6 Click **Add Organizations**.

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

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

■ Select **All organizations** to grant catalog access to all organizations in the vCloud Director installation.

■ Select **Specific organizations** to grant catalog access to certain organizations and click **Add**.

b Select the access level for users with access to this catalog from the drop-down menu and click **OK**.

■ Select **Read Only** to grant read access to the catalog's vApp templates and ISOs.

■ Select **Read/Write** to grant read access to the catalog's vApp templates and ISOs, and to allow organizations to add vApp templates and ISOs to the catalog.

■ Select **Full Control** to grant full access to the catalog's contents and settings.

7 Click **Next**.

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

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

Before selecting this option, verify that you have available storage at the transfer server location for the exported catalog.

10   (Optional) Select **Preserve identity information** to include BIOS and UUID information in the downloaded OVF package.

Enabling this option limits portability of the OVF package.

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

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

Access a Catalog

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

Prerequisites

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

Procedure

1   Click **Catalogs**.

2   In the left pane, click a catalog option.

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

Share A Catalog

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

Prerequisites

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

■   You must be the owner of the catalog.

Procedure

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

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

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

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

Option	Description
Everyone in this organization	All users and groups in the organization have access to this catalog.
Specific users and groups	Select users or groups to grant catalog access to and click **Add**.

5   Select the access level for users with access to this catalog from the drop-down menu.

Option	Description
Read Only	Users with access to this catalog have read access to the catalog's vApp templates and ISOs.
Read/Write	Users with access to this catalog have read access to the catalog's vApp templates and ISOs and can add vApp templates and ISOs to the catalog.
Full Control	Users with access to this catalog have full control of the catalog's contents and settings.

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

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

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

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

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

Identity information might not be usable in all other organizations.

7   Click **OK** to save your changes.

Change the Owner of a Catalog

An administrator can change the owner of a catalog.

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

Prerequisites

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

Procedure

1   Select **Catalog > My Organization's Catalogs**.

2   Click the **Catalogs** tab, right-click a catalog, and select **Change Owner**.

3   Select a user from the list or search for one.

You can search for a user by full name or by user name.

4   Click **OK**.

Delete a Catalog

You can delete a catalog from your organization.

Prerequisites

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

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

Procedure

1   Click **Catalog**.

2   In the left pane, click **My Organization's Catalogs**.

3   Select a catalog, right-click, and select **Delete**.

4   Click **Yes** to confirm.

The empty catalog is deleted from your organization.

Change the Properties of a Catalog

You can review and change catalog properties.

Prerequisites

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

You must be the owner of the catalog.

Procedure

1   Click **Catalog**.

2   In the left pane, click **My Organization's Catalogs**.

3   Select a catalog, right-click, and select **Properties**.

4   Review the properties in the **General**, **Sharing**, and **External Publishing** tabs.

5   Change the relevant properties and click **OK**.

Your catalog properties are updated.

Subscribe to an External Catalog Feed

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

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

Prerequisites

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

■   The system administrator must grant your organization permission to subscribe to external catalogs.

Procedure

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

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

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

4   Select the type of storage to use for this catalog feed and click **Next**.

Option	Description
Use any available storage in the organization	This catalog feed uses any available storage in the organization.
Pre-provision storage on specific storage policy	Select a virtual datacenter storage policy to use for this catalog feed and click **Add**.

5   Click **Add Members**.

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

Option	Description
Everyone in this organization	All users and groups in the organization have access to this catalog feed.
Specific users and groups	Select users or groups to which to grant catalog feed access and click **Add**.

7   Click **Add Organizations**.

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

Option	Description
All organizations	All organizations in the vCloud Director installation have access to this catalog feed.
Specific organizations	Select the organizations to which to grant catalog feed access and click **Add**.

9   Click **Next**.

10   Review the catalog feed settings and click **Finish**.

Working with Media Files

5

The catalog allows you to upload, copy, move, and edit the properties of media files.

This chapter includes the following topics:

Upload Media Files

You can upload media files to a catalog. Users with access to the catalog can use the media files to install applications on their virtual machines.

Prerequisites

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

Procedure

1   Select **Catalogs > My Organization's Catalogs**.

2   On the **Media** tab, click **Upload**.

3   Type the path to the media file path or click **Browse**, locate the file, and click **Upload**.

4   Type a name and optional description for the media file.

     This is the name that appears in vCloud Director. The name must include the appropriate file extension, such as `.iso`

5   Select the destination virtual datacenter, storage policy, and catalog.

6   Click **Upload**.

The media file is uploaded to the specified location. You can click **Launch Uploads and Downloads Progress Window** to track the progress.

Resume the Upload of a Media File

If you paused, cancelled, or interrupted the upload of a media file, you can resume it.

If you have to pause the upload or download of a media file, you can resume the upload later.

■ If you log out of vCloud Director and log in, transfer history is lost. You cannot resume the upload.

■ The default timeout for pending transfer sessions is 60 minutes. See VMware Knowledge Base article https://kb.vmware.com/kb/2149250 for information about changing this default.

■ During pending or stopped transfers, the session keep alive heartbeat kicks in every 15 minutes. To ensure that the session does not time out while tasks are paused, make sure the session timeout value is more than 15 minutes.

Prerequisites

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

Procedure

1   In the **Launch the Uploads and Downloads Progress Window**, click **Pause** or **Cancel**.

The status changes to **Stopped** in the progress window and **Waiting** in the **Media Files** page.

2   In the **Launch the Uploads and Downloads Progress Window**, click **Resume**.

The upload or download process resumes.

3   Monitor the progress in the **Launch the Uploads and Downloads Progress** window.

Copy Media Files to a Catalog

You can copy media files to another catalog.

Prerequisites

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

■ Your organization must have a catalog and virtual datacenter.

Procedure

1   Click **Catalogs**.

2   On the **Media** tab, select a media file, right-click, and select **Copy To Catalog**.

3   Type a name and description.

4   Select the destination catalog.

5   Click **OK**.

The media file is copied to and stored in the selected catalog.

Move Media Files to Another Catalog

You can move media files to another catalog in your organization.

Prerequisites

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

■ Your organization must have at least two catalogs and a virtual datacenter with available space.

Procedure

1 Click **Catalogs**.

2 Click the **Media** tab, select a media file, right-click, and select **Move To Catalog**.

3 Select a catalog.

The catalog you select must be in your organization.

4 Click **OK**.

The media file is moved to the selected catalog.

Delete Media Files

You can delete media files from your catalog.

Prerequisites

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

Procedure

1 Click **Catalogs > My Organization's Catalogs**.

2 On the **Media** tab, select a media file, right-click, select **Delete**.

3 Click **Yes**.

The media file is deleted.

Modify Media File Properties

You can review and modify some properties of a media file.

Prerequisites

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

Procedure

1 Click **Catalogs > My Organization's Catalogs**.

2 On the **Media** tab, select a media file, right-click, and select **Properties**.

3 Modify the name or description.

4 Click **OK**.

Working with vApp Templates

<div style="text-align: right; font-size: 3em;">6</div>

A vApp template is a virtual machine image that is loaded with an operating system, applications, and data. These templates ensure that virtual machines are consistently configured across an entire organization.

This chapter includes the following topics:

Open a vApp Template

You can open a vApp template to learn more about the virtual machines that it contains.

Prerequisites

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

Procedure

1   Click **Catalogs**.

2   In the left pane, click **My Organization's Catalogs**.

> **NOTE**
>
> If you are an organization administrator or system administrator, you can choose **Public Catalogs**.

3   On the **vApp Templates** tab, select a vApp template, right-click, and select **Open**.

Add a vApp Template to My Cloud

You can add a vApp template from a catalog as a vApp in **My Cloud**.

If the vApp template is based on an OVF file that includes OVF properties for customizing its virtual machines, those properties are passed to the vApp. If any of those properties are user-configurable, you can specify the values.

Prerequisites

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

- A vApp template must be available in a catalog in your organization.

Procedure

1   Click **Catalogs**.

2   In the left pane, click a catalog option.

    You can access vApp templates in your organization's shared catalogs or, if you are an organization administrator, from a public catalog.

3   On the **vApp Templates** tab, select a vApp template, right-click, and select **Add to My Cloud**.

4   Type a name and optional description for the vApp.

5   Select a virtual datacenter to add the vApp to.

6   Select the storage policies for the vApp's virtual machines to use when deployed from each virtual machine's drop-down menu.

7   Select runtime and storage lease duration from the drop-down menus.

8   Configure the networking options for the vApp.

9   (Optional) Configure vApp hardware settings.

Option	Description
VCPUs	Type the number of virtual CPUs and cores per socket for the vApp's virtual machines or leave this section unchanged to use the template's default virtual CPU configuration.
Memory	Type the amount of memory for the vApp's virtual machines or leave this section unchanged to use the template's default memory configuration.
Hard disk space	Type the hard disk space for the vApp's virtual machines or leave this section unchanged to use the template's default hard disk configuration.

10   Click **Next**.

11   (Optional) Select **Power on vApp after this wizard is finished** to power on the vApp after vApp creation is complete.

12   Review the vApp summary information and click **Finish**.

vCloud Director creates a vApp on the vApps page.

Download a vApp Template

You can download a vApp template from a catalog locally as an OVF file.

Prerequisites

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

Procedure

1   Click **Catalogs**.

2   In the left pane, click on a catalog option.

- **My Organization's Catalogs**

- **Public Catalogs**

You can download vApp templates from your organization's catalogs or, if you are an organization administrator, from a public catalog.

3   On the **vApp Templates** tab, select a vApp template, right-click, and select **Download**.

4   Navigate to the local folder where you want to save the OVF file.

5   (Optional) Select a format for the download and enter details in the Description field.

6   (Optional) Select **Preserve identity information** to include the UUIDs and MAC addresses of the vApp's virtual machines in the downloaded OVF package.

7   Click **OK**.

You can click the **View uploads and downloads** button to track the progress.

Upload an OVF Package as a vApp Template

You can upload an OVF package from remote shares and your local directory to vCloud Director as a vApp template.

vCloud Director supports the Open Virtualization Format (OVF) Specification. If you upload an OVF file that includes OVF properties for customizing its virtual machines, those properties are preserved in the vApp template.

Prerequisites

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

- For information about creating OVF packages, see the *OVF Tool User Guide* and *VMware vCenter Converter User's Guide*.

- vCloud Director does not support uploading compressed OVF files.

Procedure

1   Click **Catalogs > My Organization's Catalogs**.

2   On the **vApp Templates** tab, click the **Upload** button.

3   Type the name and path of the OVF file to upload, or click **Browse**, select the OVF file, and click **Upload**.

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

5   Select a destination virtual datacenter and catalog.

6   Click **Upload**.

You can click the **Launch Uploads and Downloads Progress Window** button to track the progress.

What to do next

Verify that VMware Tools is installed in each virtual machine in the vApp. See "Installing VMware Tools in a vApp," on page 101.

Resume the Upload of a vApp Template

If the upload process is interrupted, paused, or cancelled you can resume it.

If you have to pause the upload or download of a vApp template (in OVF form), you can resume the upload later.

■   If you log out of vCloud Director and log in, transfer history is lost. You cannot resume the upload.

■   The default timeout for pending transfer sessions is 60 minutes. See VMware Knowledge Base article https://kb.vmware.com/kb/2149250 for information about changing this default.

■   During pending or stopped transfers, the session keep alive heartbeat kicks in every 15 minutes. To ensure that the session does not time out while tasks are paused, make sure the session timeout value is more than 15 minutes.

Prerequisites

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

Procedure

1   In the **Launch Uploads and Downloads Progress Window**, click **Pause** or **Cancel**.

The status changes to **Stopped** in the progress window and **Waiting** in the **vApp Template** page.

2   In the **Launch Uploads and Downloads Progress Window**, click **Resume**.

The upload or download process resumes.

3   Monitor the progress in the **Launch Uploads and Downloads Progress Window** .

Copy a vApp Template from a Public Catalog to an Organization Catalog

You can copy a vApp template from a public catalog to your organization catalog to make it available to users in your organization.

Prerequisites

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

■   Your organization must have a catalog and virtual datacenter.

Procedure

1   Click **Catalogs**.

2   In the left pane, click **Public Catalogs**.

3   On the **vApp Templates** tab, select a vApp template, right-click, and select **Copy To Catalog**.

4   Type a name and optional description for the vApp.

5 Select a destination catalog and virtual datacenter.

Select a shared catalog to give organization users access to the template.

6 Click **OK**.

vCloud Director copies the vApp template to the organization catalog. The vApp appears on the **vApp Templates** tab in **My Organization's Catalogs**.

Copy a vApp Template Between an Organization's Catalogs

You can copy a vApp template from one catalog in your organization to another catalog in the same organization. This is useful if the catalogs are shared with different users and you want both groups of users to have access to the vApp template.

Prerequisites

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

■ Your organization must have at least two catalogs and a virtual datacenter with available space.

Procedure

1 Click **Catalogs > My Organization's Catalogs**.

2 On the **vApp Templates** tab, right-click a vApp template and select **Copy to Catalog**.

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

4 Select the destination catalog and virtual datacenter.

If you select a published catalog, the vApp template will be available to all organizations in the vCloud Director installation.

5 Click **OK**.

Move a vApp Template Between an Organization's Catalogs

You can move a vApp template from one catalog in your organization to another catalog in the same organization. This is useful if you want to move a template from a published catalog to an unpublished catalog or the reverse.

Prerequisites

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

■ Your organization must have at least two catalogs and a virtual datacenter with available space.

Procedure

1 Click **Catalogs > My Organization's Catalogs**.

2 On the **vApp Templates** tab, right-click a vApp template and select **Move To Catalog**.

3 Select a destination catalog and virtual datacenter.

If you select a published catalog, the vApp template will be available to all organizations in the system.

4 Click **OK**.

vCloud Director copies the source vApp template to the destination catalog and then deletes the source vApp template.

Delete a vApp Template

You can delete a vApp template from an organization catalog. If the catalog is published, the vApp template is also deleted from public catalogs.

Prerequisites

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

Procedure

1   Click **Catalogs > My Organization's Catalogs**.

2   On the **vApp Templates** tab, select a vApp template, right-click, and select **Delete**.

3   Click **Yes**.

The selected vApp is deleted.

Save a vApp as a vApp Template

You can save a vApp to a catalog as a vApp template.

Prerequisites

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

■   Your organization must have a catalog and a virtual datacenter with available space.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Right-click a vApp and select **Add to Catalog**.

If you select a running vApp, it is added to the catalog as a vApp template with all of its virtual machines in a suspended state.

4   Select **Overwrite catalog item** if you want the new catalog item to overwrite any existing vApp Template that has the same name.

5   Type a **Name** and optional **Description** for the vApp template.

6   Specify a **Storage lease**.

The default storage lease is configured by your organization administrator.

7   Specify how the template should be created.

Select an option.

Option	Description
Make Identical Copy	vApps that are created from this vApp template inherit the guest operating system settings specified in the template. If you select this option and guest customization is enabled, the guest operating system is personalized. IP addresses of the NICs in the template are reserved.
Customize VM Settings	Guest operating system is personalized regardless of the vApp template settings when the template is instantiated. IP addresses of the NICs in the template are released.

8　　Click **OK**.

The vApp is saved as a vApp template and appears in the specified catalog.

Modify vApp Template Properties

Prerequisites

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

Procedure

1　　Click **Catalogs > My Organization's Catalogs**.

2　　On the **vApp Templates** tab, right-click a vApp template and select **Properties**.

3　　On the **General** tab, modify the vApp template name and description.

4　　Select a vApp creation option.

This option applies when creating a vApp based on this template. It is ignored when building a vApp using individual virtual machines from this template.

Option	Description
Make identical copy	vApps that are created from this vApp template inherit the guest operating system settings specified in the template. If you select this option and guest customization is enabled, the guest operating system is personalized. IP addresses of the NICs in the template are re-used if they were reserved by specifying **Make identical copy** when the template was created.
Customize VM settings	Guest operating system is personalized regardless of the vApp template settings when the template is instantiated. IP addresses of the NICs in the template are not re-used. This option requires that a supported version of VMware Tools be installed on all virtual machines in the vApp.

5　　Choose whether or not to mark the vApp template as a Gold Master in the catalog.

If you mark a vApp template as a Gold Master, this information appears in the list of vApp templates.

6　　To reset the vApp template storage lease, select the **Reset lease** check box and select a new storage lease.

7　　Click **OK**.

Change the Guest OS Properties of a vApp Template

You can change the guest operating system properties of an existing vApp template, such as password and domain properties.

Prerequisites

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

Procedure

1　　Click **Catalogs**.

2　　In the left pane, click **My Organization's Catalogs**.

3　　Click the **vApp Templates** tab, right-click the vApp template to change and select **Open**.

4   Click the **VMs** tab, right-click the virtual machine to change and select **Properties**.

5   Click the **Guest OS Customization** tab.

6   (Optional) Change guest OS properties.

Option	Description
Guest customization.	Enables or disables guest customization.
Change SID	Runs Sysprep to change Windows SID. This option is available only for virtual machines running a Windows guest operating system.
Allow local administrator password	Allows setting an administrator password on the guest operating system.
Require administrator to change password on first login	Requires the administrator to change this password the first time they log in to the guest operating system.
Enable this VM to join a domain	Type domain properties to have the virtual machine join a domain
Browse	Navigate to a customization script, and click **OK** to add the customization script to the vApp template.

7   Click **OK**.

Working with vApps 7

A vApp consists of one or more virtual machines that communicate over a network and use resources and services in a deployed environment. A vApp can contain multiple virtual machines.

This chapter includes the following topics:

Open a vApp

You can open a vApp to view the virtual machines and networks it contains, as well as a diagram showing how the virtual machines and networks are conected.

Procedure

1   Click **My Cloud > vApps**.

2   Select a vApp, right-click, and select **Open**.

Create a vApp From a vApp Template

You can create a new vApp based on a vApp template stored in a catalog to which you have access.

- Only organization administrators and vApp authors can access vApp templates in public catalogs.

- vApp users and above can access vApp templates in organization catalogs shared to them.

If the vApp template is based on an OVF file that includes OVF properties for customizing its virtual machines, those properties are passed to the vApp. If any of those properties are user-configurable, you can specify the values.

Procedure

1   Click **My Cloud > vApps**.

2   Click the **Add vApp from Catalog** button.

3   Select **My organization's catalogs** or **Public catalogs** from the drop-down menu.

4   Select a vApp template and click **Next**.

5   Type a name and optional description for the vApp.

6   Select a runtime and storage lease and click **Next**.

7   Select a virtual datacenter, configure the virtual machines in the vApp, and click **Next**.

8   Select a storage policy for the vApp's virtual machines from the drop-down menu and click **Next**.

    If the storage policy supports IOPS allocation, a **Disk IOPS** field is displayed. You can accept the default value shown in this field or specify a desired level of disk I/O performance in the range 200-4000. For more information about IOPS, see the *vCloud Director Administrator's Guide*.

9   Configure the networking options for the vApp and click **Next**.

10   Review the vApp summary information and click **Finish**.

vCloud Director creates a vApp in **My Cloud**.

Create a New vApp

If you don't want to create a vApp based on a vApp template, you can create a new vApp using virtual machines from vApp templates, new virtual machines, or a combination of both.

You are at least a vApp author.

Procedure

1   Complete the vApp Profile on page 57

    When you create a new vApp, you must provide some basic information.

2   Add Virtual Machines to the vApp on page 57

    You can search your catalogs for virtual machines to add to the vApp or add new, blank virtual machines.

3   Configure the Virtual Machines on page 58

    Select the virtual datacenter in which this vApp is stored and runs when it's started. Name each virtual machine and select the network to which you want it to connect. You can configure additional properties for virtual machines after you complete the wizard.

4   Configure Networks on page 58

    You can determine how the vApp, its virtual machines, and its networks connect to the organization's networks.

Complete the vApp Profile

When you create a new vApp, you must provide some basic information.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps** and click the **Build New vApp** button.

3   Type a name and optional description.

4   Select a runtime and storage lease and click **Next**.

Add Virtual Machines to the vApp

You can search your catalogs for virtual machines to add to the vApp or add new, blank virtual machines.

You must be an organization administrator or vApp author to access public catalogs.

Procedure

1   To add virtual machines from vApp templates, select **My organization's catalogs** or **Public catalogs** from the drop-down menu, select one or more virtual machines, and click **Add**.

2   To add a new virtual machine, click **New Virtual Machine**, provide the required information about the virtual machine, and click **OK**.

    After you finish creating the new vApp, you can power on the new virtual machine and install an operating system.

3   Click **Next**.

Configure the Virtual Machines

Select the virtual datacenter in which this vApp is stored and runs when it's started. Name each virtual machine and select the network to which you want it to connect. You can configure additional properties for virtual machines after you complete the wizard.

Procedure

1   Select a virtual datacenter.

2   (Optional) Modify the full name and computer name of each virtual machine.

3   Select a primary NIC and network for each virtual machine.

4   Select an IP assignment method for each NIC.

    If you select **Static - Manual**, type the IP address.

5   Click **Next**.

Configure Networks

You can determine how the vApp, its virtual machines, and its networks connect to the organization's networks.

Procedure

1   Select **Show networking details**.

2   Review the network information.

3   Click **Next**.

4   Review the summary for the vApp.

5   Click **Finish**.

Import a Virtual Machine as a vApp

You can import a vSphere virtual machine to your organization as a vApp.

Prerequisites

Verify that you are at least a vApp author.

Procedure

1   Select **My Cloud** > **vApps**.

2   Click **Import from vSphere**.

3   Select a vCenter server from the drop-down menu and select a virtual machine to import.

4   Type a name and optional description for the vApp.

5   Select a virtual datacenter to which to import the vApp from the drop-down menu.

6   (Optional) Select a storage policy for the vApp from the drop-down menu.

7   Choose whether to move or copy the imported virtual machine, and click **OK**.

vCloud Director imports the vApp into **My Cloud**.

Create a vApp From an OVF Package

You can create and deploy a vApp directly from an OVF package without creating a vApp template and corresponding catalog item.

Prerequisites

Verify that you have an OVF package to upload and that you have permission to upload OVF packages and create vApps.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps** and click **Add vApp from OVF**.

3   Select the source from which to upload the OVF package and click **Next**.

Option	Action
URL	Type the URL of the OVF package to use.
Local file	Click **Browse** and navigate to the OVF package to use.

4   Review the details of the uploaded OVF and click **Next**.

5   Type a name and optional description for the vApp.

6   Select a virtual datacenter on which to store and run the vApp from the drop-down menu and click **Next**.

7   Select a storage policy for the vApp's virtual machines from the drop-down menu and click **Next**.

   If the storage policy supports IOPS allocation, a **Disk IOPS** field is displayed. You can accept the default value shown in this field or specify a desired level of disk I/O performance in the range 200-4000. For more information about IOPS, see the *vCloud Director Administrator's Guide*.

8   Select the network for the virtual machines to connect to from each virtual machine's drop-down menu and click **Next**.

9   Review the hardware settings for the virtual machines in the vApp and optionally change those configurations.

   If you change the hard disk size, you might need to configure the guest operating system after you power on the virtual machine. You can only increase hard disk size, but not decrease it.

10 Click **Next**.

11 Review the vApp's configuration and click **Finish**.

About the vApp Placement Engine

The vCloud Director placement engine determines what resources, including resource pools, datastores, and networks or network pools, on which to place the virtual machines in a vApp. The placement decision is made independently for each virtual machine in a vApp based on the requirements of that virtual machine.

The placement engine runs in the following scenarios.

■   When you create a vApp, the placement engine determines what resource pool, datastore, and network pool on which to place the vApp's virtual machines.

■   When you start a vApp, the placement engine might selectively move the vApp's virtual machines to another resource pool, datastore, or network pool if the current resource pool, datastore, or network pool lacks sufficient resources for the vApp to power on.

- When you change the storage policy of a virtual machine, the placement engine moves the virtual machine to a datastore and resource pool that support the new storage policy.

- When virtual machines are migrated to different resource pools.

The placement engine uses the following criteria to select candidate resource pools for a virtual machine.

- CPU capacity

- Memory capacity

- Number of virtual CPUs

- Hardware version supported by the host

The placement engine filters out disabled resource pools from the candidate list so that no virtual machine is created on a disabled resource pool. When possible, the placement engine places virtual machines on the same hub as other virtual machines in the organization virtual datacenter.

The placement engine uses the following criteria to select candidate datastores for a vApp and its virtual machines.

- Storage capacity

- Storage policy

The placement engine filters out disabled datastores from the candidate list so that no virtual machine is created on a disabled datastore.

The placement engine uses the network name to select candidate network pools for a vApp and its virtual machines.

After the placement engine selects a set of candidate resources, it ranks the resources and picks the best location for each virtual machine based on the CPU, virtual RAM, and storage configuration of each virtual machine.

While ranking resources, the placement engine examines the current and estimated future resource use. Estimated future use is calculated based on powered-off virtual machines currently placed on a given resource pool and their expected use after they are powered on. For CPU and memory, the placement engine looks at the current unreserved capacity, the maximum use, and the estimated future unreserved capacity. For storage, it looks at the aggregated provisioned capacity provided by the cluster that each resource pool belongs to. The placement engine then considers the weighted metrics of the current and future suitability of each resource pool.

The placement engine favors resource pools that provide the minimum of unreserved capacity for CPU and memory and free capacity for storage. It also gives lower preference to yellow clusters so that yellow clusters are only selected if no healthy cluster is available that satisfies the placement criteria.

When a virtual machine is powered on, either as part of starting a vApp or on its own, the placement engine runs to validate that the resource pool the virtual machine is assigned to has sufficient resources to support the requirements of the virtual machine. This step is necessary because the resource availability on the resource pool might have changed since the virtual machine was created on the resource pool. If the resource pool lacks sufficient capacity to power on the virtual machine, the placement engine finds another compatible resource pool on the provider virtual datacenter that satisfies the requirements of the virtual machine and places the virtual machine there. This substitution might result in the migration of the virtual machine's VMDKs to a different datastore if no suitable resource pools are connected to the datastore the VMDKs are located on.

During concurrent deployment situations when a resource pool is close to capacity, the validation of that resource pool might succeed even though the resource pool lacks the resources to support the virtual machine. In these cases, the virtual machine cannot power on. If a virtual machine fails to power on in this situation, start the power on operation again to prompt the placement engine to migrate the virtual machine to a different resource pool.

When the cluster that a resource pool belongs to is close to capacity, a virtual machine on that resource pool might still be able to power on even when no individual host has the capacity to power on the virtual machine. This happens as a result of capacity fragmentation at the cluster level. In such cases, a system administrator should migrate a few virtual machines out of the cluster so that the cluster maintains sufficient capacity.

Download a vApp as an OVF Package

You can download a vApp as an OVF package.

Prerequisites

Verify that the vApp is powered off and undeployed.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Right-click a vApp and select **Download**.

4   Type a name for the downloaded OVF package and click **Browse** to select a download destination.

5   (Optional) Select a format for the download and enter details in the Description field.

6   (Optional) Select **Preserve identity information** to include the UUIDs and MAC addresses of the vApp's virtual machines in the downloaded OVF package.

7   Click **OK**.

Start a vApp

Starting a vApp powers on all the virtual machines in the vApp that are not already powered on.

You are at least a vApp author.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right click, and select **Start**.

Start a vApp with an Older Version of VMware Tools

If a virtual machine in a vApp has an older version of VMware Tools installed and is enabled for guest customization, you might not be able to start it.

Procedure

1   Click **My Cloud**.

2   In the left pane, select **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   Select a virtual machine, right-click, and select **Properties**.

5   On the **Guest OS Customization** tab, deselect the **Enable Guest Customization** check box and click **OK**.

6   (Optional) Repeat this step for all your virtual machines.

7   Select the vApp, right-click, and select **Start**.

Stop a vApp

Stopping a vApp powers off or shuts down all the virtual machines in the vApp. You must stop a vApp before you can perform certain actions. For example, adding it to a catalog, copying it, moving it, and so on.

You can specify whether stopping a vApp powers off or shuts down its virtual machines in the vApp properties page.

Prerequisites

The vApp must be started.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Stop**.

4   Click **OK**.

Suspend a vApp

You can suspend a vApp to save its current state.

Prerequisites

The vApp is running.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Suspend**.

The vApp is stopped and is labeled as **Stopped**.

Discard the Suspended State of a vApp

You can discard the suspended state of a vApp.

Prerequisites

The vApp must be stopped and in a suspended state.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Discard Suspended State**.

4   Click **Yes**.

Reset a vApp or Virtual Machine

Resetting a virtual machine clears state (memory, cache, and so on), but the vApps and virtual machines continue to run.

Prerequisites

Your vApp is started and virtual machine is powered on.

Procedure

1　Click **My Cloud**.

2　In the left pane, select **vApps** or **VMs**.

3　Select a vApp or virtual machine, right-click, and select **Reset**.

View vApp Virtual Machines

You can access and display the virtual machines in a vApp.

Procedure

1　Click **My Cloud**.

2　In the left pane, click **vApps**.

3　Select a vApp, right-click, and select **Open**.

4　Click on the **Virtual Machines** tab.

Add a Virtual Machine to a vApp

You can add a virtual machine to a vApp.

If the virtual machine is based on an OVF file that includes OVF properties for customization, those properties are retained in the vApp. If any of those properties are user-configurable, you can specify the values in the virtual machine's properties pane after you add it to the vApp.

For information about supported network adapter types, see http://kb.vmware.com/kb/1001805.

Prerequisites

You must be an organization administrator or vApp author to access virtual machines in public catalogs.

Procedure

1　Click the **My Cloud** tab and click **vApps** in the left pane.

2　Right-click the vApp and select **Open**.

3　On the **Virtual Machines** tab, click the **Add VM** button.

4　To add virtual machines from vApp templates, select **My organization's catalogs** or **Public catalogs** from the drop-down menu, select one or more virtual machines, and click **Add**.

5　To add a new virtual machine, click **New Virtual Machine**, provide the required information about the virtual machine, and click **OK**.

After you finish creating the new vApp, you can power on the new virtual machine and install an operating system.

6　Click **Next**.

7　(Optional) Modify the full name and computer name of each virtual machine.

8　Select a primary NIC and network for each virtual machine.

9　(Optional) Select **Show network adapter type** and select a type for each NIC.

10　Select an IP assignment method for each NIC.

If you select **Static - Manual**, type the IP address.

11　Click **Next**.

12　Select **Show networking details**, review the network information, and click **Next**.

13　Review the summary for the vApp and click **Finish**.

Import a Virtual Machine to a vApp from vSphere

You can import an existing virtual machine to a vApp from vSphere

Prerequisites

Verify that you are a system administrator.

Procedure

1　Click the **My Cloud** tab and click **vApps** in the left pane.

2　Right-click the vApp and select **Open**.

3　On the **Virtual Machines** tab, click **Import from vSphere**.

4　Select the source vCenter server from the drop-down menu and select the virtual machine to import.

5　Enter a name for the imported virtual machine.

6　(Optional) Enter a description for the imported virtual machine.

7　(Optional) Select a storage policy for the imported virtual machine.

8　Choose whether to copy the virtual machine or to move it from the source vCenter server, and click **OK**.

Remove Virtual Machines from a vApp

You can remove virtual machines from a vApp.

You are at least a vApp author.

Prerequisites

The virtual machine is powered off.

Procedure

1　Click **My Cloud**.

2　In the left pane, click **vApps**.

3　Select a vApp, right-click, and select **Open**.

4　On the **Virtual Machines** tab, select a virtual machine, right-click and select **Delete**.

5　Click **Yes**.

Set vApp Start and Stop Options

You can specify certain options that affect what happens to the virtual machines when a vApp is started and stopped.

Prerequisites

You are at least a vApp user.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Properties**.

4   On the **Starting and Stopping VMs** tab, specify the options.

Option	Description
Order	For vApps with multiple virtual machines, you can specify the order in which the machines start and stop by typing numbers in the text box. Virtual machines with lower numbers start first and stop last. You cannot enter negative numbers. Virtual machines with the same order are started and stopped at the same time.
Start Action	Determines what happens to virtual machines when you start the vApp that contains them. By default, this option is set to **Power On**.
Boot Delay	How many seconds vCloud Director waits after starting the virtual machine before starting the next virtual machine.
Stop Action	Determines what happens to virtual machines when you stop the vApp that contains them. By default, this option is set to **Power Off**, but you can also set it to **Shutdown**.
Stop Delay	How many seconds vCloud Director waits after stopping the virtual machine before stopping the next virtual machine.

5   Click **OK**.

Example: Starting and Stopping Virtual Machines

This example shows a the order, boot delay, and stop delay options for the virtual machines in a vApp and how those options affect when each virtual machine starts and stops.

Table 7-1. Virtual Machine Start and Stop Options on vApp1

Virtual Machine	Order	Boot Delay	Stop Delay
VM1	1	0	10
VM2	1	10	10
VM3	1	20	30
VM4	2	0	20
VM5	2	30	60
VM6	3	40	10

When vApp1 is started, the virtual machines start as follows.

1   VM1, VM2, and VM3 start at the same time.

2   After 20 seconds (the longest boot delay from the order 1 virtual machines), VM4 and VM5 start.

3   After 30 seconds (the longest boot delay from the order 2 virtual machines) VM6 starts.

When vApp1 is stopped, the virtual machines stop as follows.

1   VM6 stops.

2   After 10 seconds, VM5 and VM4 stop.

3   After 60 seconds, VM3, VM2, and VM1 stop.

Working with Networks in a vApp

The virtual machines in a vApp can connect to vApp networks (isolated or routed) and organization virtual datacenter networks (direct or fenced). You can add networks of different types to a vApp to address multiple networking scenarios.

Select the **Networking** tab in a vApp and select the **Show networking details** check box to view a list of the networks that are available to the vApp. Virtual machines in the vApp can connect to these networks. If you want to connect a virtual machine to a different network, you must first add it to the vApp.

A vApp can include vApp networks and organization virtual datacenter networks. A vApp network can be isolated by selecting **None** in the **Connection** drop-down menu. An isolated vApp network is totally contained within the vApp. You can also route a vApp network to an organization virtual datacenter network to provide connectivity to virtual machines outside of the vApp. For routed vApp networks, you can configure network services, such as a firewall and static routing.

You can connect a vApp directly to an organization virtual datacenter network. If you have multiple vApps that contain identical virtual machines connected to the same organization virtual datacenter network and you want to start the vApps at the same time, you can fence the vApp. This allows you to power on the virtual machines without conflict, by isolating their MAC and IP addresses.

View vApp Networks

You can access and display the networks in a vApp.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   Click on the **Networking** tab.

5   Select the **Show networking details** to display details about each network.

Adding Networks to a vApp

You can add vApp networks and organization virtual datacenter networks to a vApp.

■   Add a vApp Network to a vApp on page 67

    Add a vApp network to a vApp to make the network available to virtual machines in the vApp.

■   Add an Organization Virtual Datacenter Network to a vApp on page 67

    You can add an organization virtual datacenter network to a vApp to make the network available to virtual machines in the vApp.

Add a vApp Network to a vApp

Add a vApp network to a vApp to make the network available to virtual machines in the vApp.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **vApps**, right-click, and select **Open**.

3 On the **Networking** tab, select the **Show networking details** check box.

4 Click the **Add Network** button.

5 Select **vApp Network** and click **Next**.

6 Type the network specifications and click **Next**.

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

8 Review your vApp network settings and click **Finish**.

   vCloud Director creates an isolated vApp network and displays it in the network list.

9 (Optional) Select an organization virtual datacenter network in the **Connection** drop-down menu.

   This routes the vApp network to the organization virtual datacenter network.

10 Click **Apply**.

What to do next

Connect a virtual machine in the vApp to the network.

Add an Organization Virtual Datacenter Network to a vApp

You can add an organization virtual datacenter network to a vApp to make the network available to virtual machines in the vApp.

Connections can be direct or fenced. Fencing allows identical virtual machines in different vApps to be powered on without conflict by isolating the MAC and IP addresses of the virtual machines.

When fencing is enabled and the vApp is powered on, an isolated network is created from the organization virtual datacenter's network pool. An edge gateway is created and attached to the isolated network and the organization virtual datacenter network. Traffic going to and from the virtual machines pass through the edge gateway, which translates the IP address using NAT and proxy-AR, which allows a router to pass traffic between two networks using the same IP space.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **vApps**, right-click, and select **Open**.

3 Click the **Networking** tab and select the **Show networking details** check box.

4 Click **Add Network**.

5 Select **Organization VDC Network** and click **Next**.

6 Select an organization virtual datacenter network and click **Finish**.

   vCloud Director adds the organization virtual datacenter network and displays it in the network list.

7 (Optional) Select the **Fence vApp** check box.

   The connection changes from direct to fenced for all organization virtual datacenter networks in the vApp.

8   Click **Apply**.

What to do next

Connect a virtual machine in the vApp to the network.

Configuring Network Services for a vApp Network

You can configure network services, such as DHCP, firewalls, network address translation (NAT), and static routing for certain vApp networks.

The network services available depend on the type of vApp network.

Table 7-2. Network Services Available by Network Type

vApp Network Type	DHCP	Firewall	NAT	Static Routing
Direct				
Routed	X	X	X	X
Isolated	X			

Configure DHCP for an vApp Network

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

When you enable DHCP for a vApp network, connect a NIC on virtual machine in the vApp 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.

Prerequisites

A routed vApp network or an isolated vApp network.

Procedure

1   Click the **My Cloud** tab and click **vApps** in the left pane.

2   Right-click a vApp and select **Open**.

3   On the **Networking** tab, select **Show networking details**.

4   Right-click the vApp network and select **Configure Services**.

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

6   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 vApp network.

7   Set the default lease time and maximum lease time or use the default values and click **OK**.

8   Click **Apply**.

vCloud Director updates the network to provide DHCP services.

NOTE   If the DNS settings on a DHCP-enabled vApp network are changed, the vApp network no longer provides DHCP services. To correct this issue, disable and reenable DHCP on the vApp network.

Configure the Firewall for a vApp Network

You can configure certain vApp networks to provide firewall services. Enable the firewall on a vApp network to enforce firewall rules on incoming traffic, outgoing traffic, or both.

When you enable the firewall, you can specify a default firewall action to deny all incoming and outgoing traffic or to allow all incoming and outgoing traffic. You can also add specific firewall rules to allow or deny traffic that matches the rules to pass through the firewall. These rules take precedence over the default firewall action. See "Add a Firewall Rule to a vApp Network," on page 69.

If a system administrator specified syslog server settings and those settings have been applied to the vApp network, then you can log events related to the default firewall action. For information about applying syslog server settings, see "Apply Syslog Server Settings to a vApp Network," on page 77. To view the current syslog server settings see "View Syslog Server Settings for a vApp Network," on page 76.

Prerequisites

A routed vApp network.

Procedure

1   Click the **My Cloud** tab and click **vApps** in the left pane.

2   Right-click a vApp and select **Open**.

3   On the **Networking** tab, select **Show networking details**.

4   Right-click the vApp network and select **Configure Services**.

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

6   Select the default firewall action.

Option	Description
Deny	Blocks all traffic except when overridden by a firewall rule.
Allow	Allows all traffic except when overridden by a firewall rule.

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

8   Click **OK**.

9   Click **Apply**.

Add a Firewall Rule to a vApp Network

You can add firewall rules to a vApp 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 vApp network. See "Configure the Firewall for a vApp Network," on page 69.

When you add a new firewall rule to a vApp network, it appears at the end of the firewall rule list. For information about setting the order in which firewall rules are enforced, see "Reorder Firewall Rules for a vApp Network," on page 71.

If a system administrator specified syslog server settings and those settings were applied to the vApp network, then you can log firewall rule events. For information about applying syslog server settings, see "Apply Syslog Server Settings to a vApp Network," on page 77. To view the current syslog server settings, see "View Syslog Server Settings for a vApp Network," on page 76.

Prerequisites

A routed vApp network.

Procedure

1   Click the **My Cloud** tab and click **vApps** in the left pane.

2   Right-click a vApp and select **Open**.

3   On the **Networking** tab, select **Show networking details**.

4   Right-click the vApp network and select **Configure Services**.

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

6   Type a name for the rule.

7   Type the traffic **Source**.

Option	Description
IP address	Type a source IP address to apply this rule on.
Range of IP addresses	Type a range of source IP addresses to apply this rule on.
CIDR	Type the CIDR notation of traffic to apply this rule on.
`internal`	Apply this rule to all internal traffic.
`external`	Apply this rule to all external traffic.
`any`	Apply this rule to traffic from any source.

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

9   Type the traffic **Destination**.

Option	Description
IP address	Type a destination IP address to apply this rule on.
Range of IP addresses	Type a range of destination IP addresses to apply this rule on.
CIDR	Type the CIDR notation of traffic to apply this rule on.
`internal`	Apply this rule to all internal traffic.
`external`	Apply this rule to all external traffic.
`any`	Apply this rule to traffic with any destination.

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

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

12   Select the action.

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

13   Select the **Enabled** check box.

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

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

15   Click **OK** and click **OK** again.

16   Click **Apply**.

Reorder Firewall Rules for a vApp 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 a vApp network, it appears at the bottom of the firewall rule list. If you want to enforce the new rule before an existing rule, reorder the rules.

Prerequisites

A routed vApp network with two or more firewall rules.

Procedure

1 Click the **My Cloud** tab and click **vApps** in the left pane.

2 Right-click a vApp and select **Open**.

3 On the **Networking** tab, select **Show networking details**.

4 Right-click the vApp network and select **Configure Services**.

5 Click the **Firewall** tab.

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

7 Click **OK**.

8 Click **Apply**.

Enable IP Masquerading for a vApp Network

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

Prerequisites

Verify that a routed vApp network exists.

Procedure

1 Click the **My Cloud** tab and click **vApps** in the left pane.

2 Right-click a vApp and select **Open**.

3 On the **Networking** tab, select **Show networking details**.

4 Right-click the vApp network and select **Configure Services**.

5 Click the **NAT** tab and select **Port Forwarding**.

6 Select **Enable IP Masquerade** and click **OK**.

7 Click **Apply**.

Add a Port Forwarding Rule to a vApp Network

You can configure certain vApp networks to provide port forwarding by adding a NAT mapping rule. Port forwarding provides external access to services running on virtual machines on the vApp network.

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

When you add a new port forwarding rule to a vApp network, it appears at the bottom of the NAT mapping rule list. For information about how to set the order in which port forwarding rules are enforced, see "Reorder Port Forwarding Rules for a vApp Network," on page 73.

Prerequisites

A routed vApp network.

Procedure

1 Click the **My Cloud** tab and click **vApps** in the left pane.

2 Right-click a vApp and select **Open**.

3 On the **Networking** tab, select **Show networking details**.

4 Right-click the vApp network and select **Configure Services**.

5 Click the **NAT** tab, select **Port Forwarding**, and click **Add**.

6 Configure the port forwarding rule.

    a Select an external port.

    b Select an internal port.

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

    d Select a VM interface.

    e Click **OK**.

7 Click **OK**.

8 Click **Apply**.

Add an IP Translation Rule to a vApp Network

You can configure certain vApp networks to provide IP translation by adding a NAT mapping rule.

When you create an IP translation rule for a network, vCloud Director adds a DNAT and SNAT rule to the edge gateway 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.

Prerequisites

Verify that you have a routed vApp network.

Procedure

1 Click the **My Cloud** tab and click **vApps** in the left pane.

2 Right-click a vApp and select **Open**.

3 Click the **Networking** tab and select **Show networking details**.

4 Right-click the vApp network and select **Configure Services**.

5 Click the **NAT** tab, select **IP Translation**, and click **Add**.

6 Select a virtual machine interface and mapping mode and click **OK**.

    For **Manual** mapping mode, type an external IP address.

7 If you select manual mapping mode, type an external IP address.

8 Click **OK**.

9   Click **Apply**.

Reorder Port Forwarding Rules for a vApp Network

Port forwarding rules are enforced in the order in which they appear in the NAT mapping list. You can change the order of the rules in the list.

When you add a new port forwarding rule to a vApp network, it appears at the bottom of the NAT mapping rule list. To enforce the new rule before an existing rule, reorder the rules.

Prerequisites

A routed vApp network with two or more port forwarding rules.

Procedure

1   Click the **My Cloud** tab and click **vApps** in the left pane.

2   Right-click a vApp and select **Open**.

3   On the **Networking** tab, select **Show networking details** and click **Details**.

4   On the **NAT** tab, click and drag the rules to establish the order in which the rules are applied and click **OK**.

5   Click **Apply**.

Enable Static Routing for a vApp Network

You can configure certain vApp networks to provide static routing services. After you enable static routing on two or more vApp networks, you can add static routes to allow virtual machines on different vApp networks to communicate.

To route traffic between two vApp networks, you must enable static routing on both networks.

Prerequisites

A routed vApp network.

Procedure

1   Click the **My Cloud** tab and click **vApps** in the left pane.

2   Right-click a vApp and select **Open**.

3   On the **Networking** tab, select **Show networking details**.

4   Right-click the vApp network and select **Configure Services**.

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

6   Click **Apply**.

What to do next

Enable static routing on another vApp network and create static routes between the two vApp networks.

Add Static Routes to vApp Networks

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

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

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

Prerequisites

Verify that the following conditions are met.

■ Two vApp networks are routed to the same organization virtual datacenter network.

■ The vApp networks are in vApps that were started at least once.

■ Static routing is enabled on both vApp networks.

Procedure

1 Click the **My Cloud** tab and click **vApps** in the left pane.

2 Right-click the first vApp and select **Open**.

3 Click the **Networking** tab and select **Show networking details**.

4 Right-click the vApp network and select **Configure Services**.

5 Click the **Static Routing** tab and click **Add**.

6 Type a name, network address, and next hop IP and click **OK**.

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

7 Click **OK**.

8 Click **Apply**.

9 Repeat Step 2 through Step 8 for 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 a static route on each vApp network to allow traffic between the networks. You can use information about the vApp networks to create the static routes.

Table 7-3. 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 vApp Network 1, create a static route to vApp Network 2. On vApp Network 2, create a static route to vApp Network 1.

Table 7-4. Static Routing Settings

vApp Network	Route Name	Network	Next Hop IP Address
vApp Network 1	tovapp2	192.168.2.0/24	192.168.0.101
vApp Network 2	tovapp1	192.168.1.0/24	192.168.0.100

What to do next

Create firewall rules for the vApp networks to allow traffic on the static routes.

Reset Your vApp Network

If the network services, such as DHCP settings, firewall settings, and so on, that are associated with a vApp network are not working as expected, an organization administrator can reset the network. Network services are not available during the reset.

Prerequisites

The vApp is running.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   On the **Networking** tab, select the **Show networking details** check box.

5   Select a vApp network, right-click, and select **Reset Network**.

6   Click **Yes**.

Delete a vApp Network

If you no longer need a network in your vApp, you can delete the network.

Prerequisites

The vApp is stopped and no virtual machines in the vApp are connected to the network.

Procedure

1   Click **My Cloud**.

2   In the left pane, select **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   On the **Networking** tab, select the **Show networking details** check box.

5   Right-click a network in the list and select **Delete**.

6   Click **Apply**.

Modify Network Properties

You can modify the properties of the networks in a vApp.

Procedure

1   Select **Administration**.

2   Select **Cloud Resources > Networks**.

3   Select a network, right-click, and select **Properties**.

You can modify the name, description, and portions of the network specification.

4   Modify the relevant properties and click **OK**.

5   Click **Apply**.

Display the IP Allocations for Your vApp Network

You can review the IP allocations for the networks in your vApp.

Procedure

1   Click **My Cloud**.

2   In the left pane, select **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   On the **Networking** tab, select the **Show networking details** check box.

5   Select a network, right-click, and select **IP Allocations**.

6   Review your allocations and click **OK**.

Configure IP Address Persistence

By default, when you stop a running vApp, vCloud Director releases any IP address the edge gateway was using. You can configure a vApp network to retain the IP addresses of its edge gateway until the vApp or network is deleted.

This setting applies only to fenced and routed vApp networks.

Static routing relies on the IP address of the edge gateway in a vApp. For vApps that use static routing, enable IP persistence to make sure that static routes to and from the vApp remain valid.

Procedure

1   Click **My Cloud**.

2   In the left pane, select **vApps**.

3   Right-click a vApp, and select **Open**.

4   On the **Networking** tab, choose which fenced or routed vApp networks should retain their IP addresses.

5   Select **Always use assigned IP addresses...** , and click **Apply**.

The edge gateways in the vApp keep their assigned IP addresses, even when they are powered off.

View Syslog Server Settings for a vApp Network

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

vCloud Director supports logging events related to firewall rules to a syslog server specified by a system administrator.

If a vApp network does not have any syslog server settings and you think it should, or if the settings are not what you expected, then you can synchronize the network with the most current syslog server settings. See If there is still a problem after you synchronize, contact your system administrator.

Prerequisites

A routed vApp network.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   On the **Networking** tab, select a vApp network, right-click, and select **Properties**.

5   Click the **Syslog Server Settings** tab.

Apply Syslog Server Settings to a vApp Network

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

Syslog server settings can only be specified by a system administrator. You should apply those settings to any vApp network that was created before the system administrator specified them. You should also apply the syslog server settings to a vApp network any time a system administrator changes the settings.

Prerequisites

A routed vApp network.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   On the **Networking** tab, select a vApp network, right-click, and select **Synchronize syslog server settings**.

5   Click **Yes**.

Editing vApp Properties

You can edit the properties of an existing vApp, including the vApp name and description, OVF environment properties, leases, and sharing settings.

- Modify a vApp Name and Description on page 77

  You can change the name and description associated with a vApp to make it more meaningful.

- Modify vApp OVF Environment Properties on page 78

  If a vApp includes user-configurable OVF environment properties, you can review and modify those properties.

- Reset vApp Leases on page 78

  You can reset the runtime and storage leases for a vApp.

- Share a vApp on page 78

  You can share your vApps with other groups or users in your organization. The access controls you set determine the operations that can be completed on the shared vApps.

Modify a vApp Name and Description

You can change the name and description associated with a vApp to make it more meaningful.

You are at least a vApp user.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Properties**.

4   On the **General** tab, modify the vApp name and description and click **OK**.

Modify vApp OVF Environment Properties

If a vApp includes user-configurable OVF environment properties, you can review and modify those properties.

If a virtual machine in the vApp includes a value for a user-configurable property of the same name, the virtual machine value takes precedence.

Prerequisites

The vApp is stopped and its OVF environment includes user-configurable properties.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Properties**.

4   On the **Custom Properties** tab, modify the properties and click **OK**.

Reset vApp Leases

You can reset the runtime and storage leases for a vApp.

You are at least a vApp user.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Properties**.

4   On the **General** tab, select the **Reset leases** check box, select a runtime and storage lease, and click **OK**.

Share a vApp

You can share your vApps with other groups or users in your organization. The access controls you set determine the operations that can be completed on the shared vApps.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Share**.

4   Click **Add Members**.

5   Select the users with whom you want to share the vApp.

Option	Action
Everyone in the organization	Select this option.
Specific users and group	Select this option, select the users and groups, and click **Add**.

6   Select an access level for the users and groups.

Option	Description
Full control	Users can open, start, save a vApp as a vApp template (**Add to Catalog**), change the owner, copy to a catalog, and modify properties.
Read/write	Users can open, start, save a vApp as a vApp template (**Add to Catalog**), copy to catalog, and modify properties.
Read only	Users only have read access to a vApp.

7   Click **OK**.

Your vApp is shared with the specified users or groups.

Display a vApp Diagram

A vApp diagram provides a graphical view of the virtual machines and networks in a vApp.

Procedure

1   Click **My Cloud**.

2   On the **vApps** page, select a vApp, right-click, and select **Open**.

3   Click the **vApp Diagram** tab.

The vApp diagram is displayed.

What to do next

You can perform most of the same operations from this tab that you can from the **Virtual Machines** and **Networking** tabs.

Change the Owner of a vApp

You can change the owner of the vApp, for example, if a vApp owner leaves the company or changes roles within the company.

You are an organization administrator.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Change Owner**.

4   Search for a user or select one from the list.

You can search by user name or full name.

5   Click **OK**.

The new owner's name appears in the **Owner** column on the **vApp** page.

Upgrade the Virtual Hardware Version for a vApp

You can upgrade the virtual hardware version for all the virtual machines in a vApp. Higher virtual hardware versions support more features.

vCloud Director supports hardware version 4, hardware version 7, hardware version 8, hardware version 9, and hardware version 10 virtual machines depending on the resources backing the organization's virtual datacenters.

You cannot downgrade the hardware version of the virtual machines in a vApp.

Prerequisites

The vApp must be stopped and its virtual machines must have the latest version of VMware Tools installed.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Upgrade Virtual Hardware Version**.

4   Click **Yes**.

Save vApp as a vApp Template to Your Catalog

You can save a vApp as a vApp template and add it to the catalog.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Add to Catalog**.

4   (Optional) Modify the name and description.

5   Select the destination virtual datacenter and catalog.

6   In the **Storage lease:** drop-down menu, select when you would like the vApp template to expire.

7   Specify how the template should be created.

   Select an option.

Option	Description
Make Identical Copy	vApps that are created from this vApp template inherit the guest operating system settings specified in the template. If you select this option and guest customization is enabled, the guest operating system is personalized. IP addresses of the NICs in the template are reserved.
Customize VM Settings	Guest operating system is personalized regardless of the vApp template settings when the template is instantiated. IP addresses of the NICs in the template are released.

8   Click **OK**.

The vApp is saved as a vApp template in the selected catalog.

Save a Powered-On vApp to your Catalog

You can save a powered-on vApp as a vApp template and add it to the catalog.

You do not need to power off virtual machines in the vApp before you save the vApp to a catalog. The memory state of running virtual machines is preserved in the saved vApp.

Prerequisites

Verify that the following conditions are met.

- You are at least a vApp user.

- The organization virtual datacenter is backed by vCenter Server 5.5.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **vApps**.

3 Select a vApp, right-click, and select **Add to Catalog**.

4 (Optional) Modify the name and description.

5 Select the destination catalog.

6 In the **Storage lease** drop-down menu, select when the vApp template should expire.

7 Specify how the template should be created.

Select an option.

Option	Description
Make Identical Copy	vApps that are created from this vApp template inherit the guest operating system settings specified in the template. If you select this option and guest customization is enabled, the guest operating system is personalized. IP addresses of the NICs in the template are reserved.
Customize VM Settings	Guest operating system is personalized regardless of the vApp template settings when the template is instantiated. IP addresses of the NICs in the template are released.

8 Click **OK**.

The vApp is added to the catalog in a suspended mode. The added vApp is enabled for network fencing.

What to do next

Modify the network properties of the vApp or power on the vApp.

Create a Snapshot of a vApp

You can take a snapshot of all the virtual machines in a vApp. After you take the snapshots, you can revert all virtual machines in the vApp to the most recent snapshot, or remove all snapshots.

vApp snapshots have the following limitations.

- They do not capture NIC configurations.

- You cannot create them if any virtual machine in the vApp is connected to an independent disk.

Procedure

1 Select **My Cloud** > **vApps**.

2   Right-click the vApp and select **Create Snapshot**.

3   Click **OK**.

Revert a vApp to a Snapshot

You can revert all virtual machines in a vApp to the state they were in when the vApp snapshot was created.

Prerequisites

Verify that the vApp has a snapshot.

Procedure

1   Select **My Cloud** > **vApps**.

2   Right-click the vApp and select **Revert to Snapshot**.

3   Click **Yes**.

Remove a Snapshot of a vApp

You can remove a snapshot of a vApp.

Procedure

1   Select **My Cloud > vApps**.

2   Right-click the vApp and select **Remove Snapshot**.

3   Click **Yes**.

Copy a vApp to Another Virtual Datacenter

When you copy a vApp to another virtual datacenter, the original vApp remains in the source virtual datacenter.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Copy to**.

4   Type a name and description.

5   Select a virtual datacenter.

6   Click **OK**.

The new virtual datacenter for this vApp appears in the **VDC** column on the **vApps** page.

Copy a Powered-On vApp

To create a vApp based on an existing vApp, you can copy a vApp and change the copy to meet your needs.

You do not need to power off virtual machines in the vApp before you copy the vApp. The memory state of running virtual machines is preserved in the copied vApp.

Prerequisites

Verify that the following conditions are met.

■   You are at least a vApp user.

■　The organization virtual datacenter is backed by vCenter Server 5.5.

Procedure

1　Click **My Cloud**.

2　In the left pane, click **vApps**.

3　Select a vApp, right-click, and select **Copy to**.

4　Type a name and optional description.

5　Select a virtual datacenter.

6　Select a storage policy from the drop-down menu.

7　Click **OK**.

A copy of the vApp is created in a suspended mode. The copied vApp is enabled for network fencing.

What to do next

Modify the network properties of the new vApp or power on the vApp.

Move a vApp to Another Virtual Datacenter

When you move a vApp to another virtual datacenter, the vApp is removed from the source virtual datacenter.

You are at least a vApp author.

Prerequisites

Your vApp is stopped.

Procedure

1　Click **My Cloud**.

2　In the left pane, click **vApps**.

3　Select a vApp, right-click, and select **Move to**.

4　Select a **VDC**.

5　Click **OK**.

Delete a vApp

You can delete a vApp, which removes it from your organization.

You must be at least a vApp author.

Prerequisites

Your vApp must be stopped.

Procedure

1　Click **My Cloud**.

2　In the left pane, click **vApps**.

3　Select a vApp, right-click, and select **Delete**.

4　Click **Yes**.

Working with Virtual Machines 8

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. The virtual machine consists of a set of specification and configuration files and is backed by the physical resources of a host. Every virtual machine has virtual devices that provide the same functionality as physical hardware are more portable, more secure, and easier to manage.

In addition to the kinds of operations that you can execute on a physical machine, vCloud Director virtual machines support virtual infrastructure operations such as moving a virtual machine from one host to another, taking a snapshot of virtula machine state, and establishing affinity between virtual machines that have similar requirements

This chapter includes the following topics:

Open a Virtual Machine Console

Accessing your virtual machine console allows you to view information about a virtual machine, work with the guest operating system, and perform operations that affect the guest operating system.

You might be required to download and install the VMware Remote Console application. Click **OK** in the dialog box that appears.

Prerequisites

The virtual machine is powered on.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Popout Console**.

   If you close or refresh a virtual machine console while you have one or more client devices connected, those devices are disconnected.

Power On a Virtual Machine

Powering on a virtual machine is the equivalent of powering on a physical machine.

You cannot power on a virtual machine that has guest customization enabled unless the virtual machine has a current version of VMware Tools installed.

Prerequisites

A virtual machine that is powered off.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Power On**.

Power Off a Virtual Machine

Powering off a virtual machine is the equivalent of powering off a physical machine.

Prerequisites

A virtual machine that is powered on.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Power Off**.

Reset a vApp or Virtual Machine

Resetting a virtual machine clears state (memory, cache, and so on), but the vApps and virtual machines continue to run.

Prerequisites

Your vApp is started and virtual machine is powered on.

Procedure

1   Click **My Cloud**.

2   In the left pane, select **vApps** or **VMs**.

3   Select a vApp or virtual machine, right-click, and select **Reset**.

Suspend a Virtual Machine

Suspending a virtual machine preserves its current state.

Prerequisites

A virtual machine that is powered on.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Suspend**.

4   Click **Yes**.

Resume a Suspended Virtual Machine

You can resume a suspended virtual machine to power it on and return it to the state it was in when you suspended it.

Prerequisites

A suspended virtual machine.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Resume**.

Discard the Suspended State of a Virtual Machine

If a virtual machine is in a suspended state, you can discard this state, for example, to free storage space.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Discard Suspended State**.

4   Click **Yes**.

Insert a CD/DVD

You can access CD/DVD images from catalogs to use in a virtual machine guest operating system. You can install operating systems, applications, drivers, and so on.

Prerequisites

You have access to a catalog with media files.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   In the right pane, select a virtual machine, right-click, and select **Insert CD/DVD from Catalog**.

4   Select a media file and click **Insert**.

The selected CD or DVD is inserted.

Eject a CD/DVD

After you have finished using a CD or DVD in your virtual machine you can eject it.

Procedure

1   Click **My Cloud**.

2   In the left pane, select **VMs**.

3   Select a virtual machine, right-click, and select **Eject CD/DVD**.

The media file is removed from the virtual machine.

Upgrade the Virtual Hardware Version for a Virtual Machine

You can upgrade the virtual hardware version for a virtual machine. Higher virtual hardware versions support more features.

The set of virtual hardware versions to which you can upgrade a VM depends on the host on which the VM is deployed. See the *vCloud Director Release Notes* for the list of virtual hardware versions supported by this release.

You cannot downgrade the hardware version of a virtual machine.

Prerequisites

Verify that the virtual machine is powered off and that it has the latest version of VMware Tools installed.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Upgrade Virtual Hardware Version**.

4   Click **Yes**.

Connect Remotely to a Virtual Machine

You can use the `Remote Desktop Connection` file to connect to a deployed virtual machine from your desktop.

Prerequisites

■ The virtual machine must be powered on, running a Windows guest OS, and have **Remote Desktop** enabled in the guest OS.

■ The virtual machine must have an IP assigned on its network that is accessible by the client.

■ The RDP port 3389 must be open on the guest OS.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Download Windows Remote Desktop Shortcut File**.

4 In the **Download RDP Shortcut File** dialog box, click **Yes**.

5 Navigate to the location where you want to save the file and click **Save**.

6 Double-click the file and select **Connect**.

Create a Snapshot of a Virtual Machine

You can take a snapshot of a virtual machine. After you take the snapshot, you can revert all the virtual machines to the most recent snapshot, or remove the snapshot.

Snapshots do not capture NIC configurations.

Prerequisites

Verify that the virtual machine is not connected to an independent disk.

Procedure

1 Select **My Cloud > VMs**.

2 Right-click the vApp and select **Create Snapshot**.

3 Click **OK**.

A snapshot of the virtual machine's state is saved. This doubles the virtual machine's storage consumption on the organization virtual datacenter.

Revert a Virtual Machine to a Snapshot

You can revert a virtual machine to the state it was in when the snapshot was created.

Prerequisites

Verify that the virtual machine has a snapshot.

Procedure

1 Select **My Cloud > VMs**.

2 Right-click the vApp and select **Revert to Snapshot**.

3 Click **Yes**.

Remove a Snapshot of a Virtual Machine

You can remove a snapshot of a virtual machine.

Procedure

1   Select **My Cloud > VMs**.

2   Right-click the vApp and select **Remove Snapshot**.

3   Click **Yes**.

Copy or Move a Virtual Machine to a vApp

You can copy or move a virtual machine to another vApp. When you copy a virtual machine, the original virtual machine remains in the source vApp. If you move a virtual machine, it is removed from the source vApp.

Prerequisites

The virtual machine must be powered off.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Copy to** or **Move to**.

4   Follow the prompts to complete the wizard.

5   Click **Finish**.

Delete a Virtual Machine

You can delete a virtual machine from your organization.

Prerequisites

Your virtual machine must be powered off.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Delete**.

4   Click **Yes**.

Virtual Machine Affinity and Anti-Affinity

Affinity and anti-affinity rules allow you to spread a group of virtual machines across different hosts or keep a group of virtual machines on a particular host.

An affinity rule places a group of virtual machines on a specific host so you can easily audit the usage of those virtual machines. An anti-affinity rule places a group of virtual machines across different hosts, which prevents all virtual machines from failing at once in the event that a single host fails.

- View Affinity and Anti-Affinity Rules on page 91

  You can view existing affinity and anti-affinity rules and their properties, such as the virtual machines affected by the rules and whether the rules are enabled.

- Add an Affinity Rule on page 91

  Add an affinity rule to place a specific group of virtual machines on a single host so you can audit the usage of those virtual machines.

- Add an Anti-Affinity Rule on page 92

  Add an anti-affinity rule to place a specific group of virtual machines across multiple hosts to prevent simultaneous failure of those virtual machines in the event that a single host fails.

- Edit an Affinity or Anti-Affinity Rule on page 92

  Edit an affinity or anti-affinity rule to enable or disable the rule, add or remove virtual machines, or change the rule's name.

- Delete an Affinity or Anti-Affinity Rule on page 92

  You can delete an existing affinity or anti-affinity rule if you no longer want to use it.

View Affinity and Anti-Affinity Rules

You can view existing affinity and anti-affinity rules and their properties, such as the virtual machines affected by the rules and whether the rules are enabled.

Procedure

1 Click **My Cloud**.

2 Click **VMs** in the left pane and click the **Affinity Rules** tab.

vCloud Director displays a list of existing affinity and anti-affinity rules and the status, virtual machines, and enabled status of each rule.

Add an Affinity Rule

Add an affinity rule to place a specific group of virtual machines on a single host so you can audit the usage of those virtual machines.

Procedure

1 Click **My Cloud**.

2 Click **VMs** in the left pane and click the **Affinity Rules** tab.

3 In the **Affinity Rules** section, click the **New Rule** button.

4 Type a **Rule Name** for the new affinity rule.

5 (Optional) Type a virtual machine name or partial virtual machine name and click the blue arrow button to filter the **Virtual Machines** list.

6 Select a virtual machine to add to the affinity rule and click **Add**.

   Repeat this step to add additional virtual machines to the rule.

7 (Optional) Deselect **Enabled** to create the rule without enabling it.

8 Click **OK** to create the new rule.

vCloud Director places the virtual machines associated with the affinity rule on a single host.

Add an Anti-Affinity Rule

Add an anti-affinity rule to place a specific group of virtual machines across multiple hosts to prevent simultaneous failure of those virtual machines in the event that a single host fails.

Procedure

1   Click **My Cloud**.

2   Click **VMs** in the left pane and click the **Affinity Rules** tab.

3   In the **Anti-Affinity Rules** section, click the **New Rule** button.

4   Type a **Rule Name** for the new affinity rule.

5   (Optional) Type a virtual machine name or partial virtual machine name and click the blue arrow button to filter the **Virtual Machines** list.

6   Select a virtual machine to add to the affinity rule and click **Add**.

    Repeat this step to add additional virtual machines to the rule.

7   (Optional) Deselect **Enabled** to create the rule without enabling it.

8   Click **OK** to create the new rule.

vCloud Director places the virtual machines associated with the anti-affinity rule across multiple hosts.

Edit an Affinity or Anti-Affinity Rule

Edit an affinity or anti-affinity rule to enable or disable the rule, add or remove virtual machines, or change the rule's name.

Procedure

1   Click **My Cloud**.

2   Click **VMs** in the left pane and click the **Affinity Rules** tab.

3   Right click the rule to modify, and select **Edit Rule**.

4   (Optional) Type a new **Rule Name** to rename the rule.

5   (Optional) Select a virtual machine from the top **Virtual Machines** list and click **Add** to add the selected virtual machine to the rule.

    Repeat this step to add multiple virtual machines.

6   (Optional) Select a virtual machine from the bottom **Virtual Machines** list and click **Remove** to remove the selected virtual machine from the rule.

    Repeat this step to remove multiple virtual machines.

7   (Optional) Select **Enabled** to enable the rule or deselect **Enable** to disable the rule.

8   Click **OK** to apply the changes to the rule.

Delete an Affinity or Anti-Affinity Rule

You can delete an existing affinity or anti-affinity rule if you no longer want to use it.

Procedure

1   Click **My Cloud**.

2   Click **VMs** in the left pane and click the **Affinity Rules** tab.

3   Right-click the rule to delete and select **Delete Rule**.

vCloud Director deletes the affinity or anti-affinity rule.

Editing Virtual Machine Properties

You can edit the properties of a virtual machine, including the virtual machine name and description, CPU and memory settings, and OVF environment settings.

- Change Virtual Machine General Properties on page 93

  You can review and change the name, description, and other general properties of a virtual machine.

- Change Virtual Machine CPU, Memory, and Disk-Level Storage Policies on page 94

  You can change virtual machine hardware, such as CPU, memory, hard disks, disk-level storage policies, and NICs.

- Change Virtual Machine Guest OS Customization Properties on page 95

  Guest OS customization on vCloud Director is optional for all platforms. It is required for VMs that must join a Windows domain.

- Configuring Virtual Machine Resource Allocation Settings on page 96

  Reservation pool virtual datacenters support the ability to control resource allocation at the virtual machine level. Users with the necessary rights can customize the amount of resources that are allocated to their virtual machines.

- Modifying Virtual Machine Hard Disks on page 98

  You can add hard disks, edit hard disks, and delete hard disk from a virtual machine.

- Modifying Virtual Machine Network Interfaces on page 99

  You can modify virtual machine network settings, reset a MAC address, add a network interface, and delete a network interface.

Change Virtual Machine General Properties

You can review and change the name, description, and other general properties of a virtual machine.

Prerequisites

Verify that the virtual machine is powered off.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Properties**.

4   Click the **General** tab, change the properties, and click **OK**.

Option	Action
Computer name	Type the computer and host name set in the guest operating system that identifies the virtual machine on a network. This field is restricted to 15 characters because of a Windows OS limitation on computer names.
Description	Type an optional description of the virtual machines.
Operating System Family	Select an operating system family from the drop-down menu.
Operating System	Select an operating system from the drop-down menu.
Virtual hardware version	Virtual hardware version of the virtual machine. Select the **Upgrade to** and select a hardware version to upgrade the virtual machine hardware.

Option	Action
Virtual CPU hot add	Select the check box to enable virtual CPU hot add. This option allows you to add virtual CPUs to a powered on virtual machine. This feature is only supported on certain guest operating systems and virtual machine hardware versions.
Memory hot add	Select the check box to enable memory hot add. This option allows you to add memory to a powered on virtual machine. This feature is only supported on certain guest operating systems and virtual machine hardware versions.
Synchronize time	Select the check box to enable time synchronization between the virtual machine guest operating system and the virtual datacenter in which it is running.
Storage Policy	Select a storage policy for the virtual machine to use from the drop-down menu.

Change Virtual Machine CPU, Memory, and Disk-Level Storage Policies

You can change virtual machine hardware, such as CPU, memory, hard disks, disk-level storage policies, and NICs.

The number of virtual CPUs and memory that a virtual machine supports depends on its virtual hardware version.

Table 8-1. Virtual Hardware Versions and CPU and Memory Support

Virtual Hardware Version	Maximum CPUs	Maximum Memory
HW4	4	64GB
HW7	8	255GB
HW8	32	1011GB
HW9	64	1011GB
HW10	64	1011GB

Prerequisites

If CPU hot add or memory hot add is not enabled for the virtual machine, power off the virtual machine before you change the CPU or memory.

Power off the virtual machine before you change the storage policy for a virtual machine disk.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Properties**.

4 Click the **Hardware** tab.

5 (Optional) Select the number of CPUs and cores per socket for the virtual machine.

6 (Optional) Select **Expose hardware-assisted CPU virtualization to guest OS** to support virtualization servers or 64-bit virtual machines running on the virtual machine.

7 (Optional) Select the total memory for the virtual machine from the **Total memory** drop-down menu.

8 (Optional) Select the storage policy for each virtual machine hard disk from the storage policy drop-down menu.

9 Click **OK**.

Change Virtual Machine Guest OS Customization Properties

Guest OS customization on vCloud Director is optional for all platforms. It is required for VMs that must join a Windows domain.

Some of the information requested on this tab applies only to Windows platforms. The **Guest OS Customization** tab includes the information necessary for the VM to join a Windows domain. An organization administrator can specify default values for a domain that Windows guests in that organization can join. Not all Windows VMs must join a domain, but in most enterprise installations, a VM that is not a domain member cannot access many network resources. For more information, see "Understanding Guest Customization," on page 112.

Prerequisites

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

■ Guest customization requires the VM to be running VMware Tools.

■ Before you can customize a Windows guest OS, your system administrator must install the appropriate Microsoft Sysprep files on vCloud Director server group. See the *vCloud Director Installation and Upgrade Guide*.

■ Customization of Linux guest operating systems requires that Perl is installed in the guest.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Properties**.

4 Click the **Guest OS Customization** tab and select **Enable guest customization**.

5 (Optional) Select **Change SID** to change the Windows SID of the VM at deployment.

This option is available only for virtual machines running a Windows guest operating system. A Windows Security ID (SID) is used in some Windows operating systems to uniquely identify systems and users. If you do not select this option, the new virtual machine has the same SID as the virtual machine or template on which it is based. Duplicate SIDs do not cause problems when the computers are part of a domain and only domain user accounts are used. However, if the computers are part of a Workgroup or local user accounts are used, duplicate SIDs can compromise file access controls. For more information, see the documentation for your Microsoft Windows operating system.

6 (Optional) Select **Allow local administrator password** to allow setting an administrator password on the guest operating system.

Option	Description
Auto generate password	vCloud Director generates an administrator password for the guest operating system.
Specify password	Type an administrator password for the guest operating system.

Select **Automatically log on as Administrator** to configure the VM to automatically log users in to the local administrator account. This option can be useful f you restart the guest operating system frequently and want to avoid entering your login credentials or you want to grant users access to the guest operating system without sharing the local administrator password.

7 (Optional) Select **Require administrator to change password on first login** to require the administrator to change this password the first time they log in to the guest operating system.

8   (Optional) Click **Enable this VM to join a domain** and type domain properties to have the virtual machine join a Windows domain.

You must select **Change SID** in Step 5 to enable the VM to join a domain.

Option	Description
Use organization's domain	The VM joins the domain configured by your organization administrator. You do not need to supply any more information.
Override organization's domain	The VM joins another domain. You must supply the domain name, domain administrator password, and account organizational unit. Syntax for the organizational unit varies with the domain. Ask your domain administrator.

9   (Optional) Upload a guest customization script.

A customization script cannot contain more than 1500 characters. You can create the script in a file on your computer, or type it directly into the **Script** window. For more information, see VMware Knowledge Base article https://kb.vmware.com/kb/1026614.

Option	Description
Script file	Click **Browse**, navigate to a customization script on your computer. When you select a file, the contents appear in the **Script** window. You can edit them in that window if you want to.
Script	Type the script in the **Script** window.

10   Click **OK** to save your changes.

Configuring Virtual Machine Resource Allocation Settings

Reservation pool virtual datacenters support the ability to control resource allocation at the virtual machine level. Users with the necessary rights can customize the amount of resources that are allocated to their virtual machines.

Use the resource allocation settings (shares, reservation, and limit) to determine the amount of CPU, memory, and storage resources provided for a virtual machine. Users have several options for allocating resources.

- Ensure that a certain amount of memory for a virtual machine is provided by the virtual datacenter.

- Guarantee that a particular virtual machine is always allocated a higher percentage of the virtual datacenter resources than other virtual machines.

- Set an upper bound on the resources that can be allocated to a virtual machine.

Resource Allocation Shares

Shares specify the relative importance of a virtual machine within a virtual datacenter. If a virtual machine has twice as many shares of a resource as another virtual machine, it is entitled to consume twice as much of that resource when these two virtual machines are competing for resources.

Shares are typically specified as **High**, **Normal**, or **Low** and these values specify share values with a 4:2:1 ratio, respectively. You can also select **Custom** to assign a specific number of shares (which expresses a proportional weight) to each virtual machine.

When you assign shares to a virtual machine, you always specify the priority for that virtual machine relative to other powered-on virtual machines.

The following table shows the default CPU and memory share values for a virtual machine.

Table 8-2. Share Values

Setting	CPU share values	Memory share values
High	2000 shares per virtual CPU	20 shares per megabyte of configured virtual machine memory.
Normal	1000 shares per virtual CPU	10 shares per megabyte of configured virtual machine memory.
Low	500 shares per virtual CPU	5 shares per megabyte of configured virtual machine memory.

For example, a virtual machine with two virtual CPUs and 1GB RAM with CPU and memory shares set to **Normal** has 2x1000=2000 shares of CPU and 10x1024=10240 shares of memory.

The relative priority represented by each share changes when a new virtual machine is powered on. This affects all virtual machines in the same virtual datacenter.

Resource Allocation Reservation

A reservation specifies the guaranteed minimum allocation for a virtual machine.

vCloud Director allows you to power on a virtual machine only if there are enough unreserved resources to satisfy the reservation of the virtual machine. The virtual datacenter guarantees that amount even when its resources are heavily loaded. The reservation is expressed in concrete units (megahertz or megabytes).

For example, assume you have 2GHz available and specify a reservation of 1GHz for VM1 and 1GHz for VM2. Now each virtual machine is guaranteed to get 1GHz if it needs it. However, if VM1 is using only 500MHz, VM2 can use 1.5GHz.

Reservation defaults to 0. You can specify a reservation if you need to guarantee that the minimum required amounts of CPU or memory are always available for the virtual machine.

Resource Allocation Limit

Limit specifies an upper bound for CPU and memory resources that can be allocated to a virtual machine.

A virtual datacenter can allocate more than the reservation to a virtual machine, but never allocates more than the limit, even if there are unused resources on the system. The limit is expressed in concrete units (megahertz or megabytes).

CPU and memory resource limits default to unlimited. When the memory limit is unlimited, the amount of memory configured for the virtual machine when it was created becomes its effective limit in most cases.

In most cases, it is not necessary to specify a limit. You might waste idle resources if you specify a limit. The system does not allow a virtual machine to use more resources than the limit, even when the system is underutilized and idle resources are available. Specify a limit only if you have good reasons for doing so.

Configure Virtual Machine Resource Allocation Settings

You can configure the resource allocation settings (shares, reservation, and limit) to determine the amount of CPU, memory, and storage resources provided for a virtual machine.

For more information about shares, reservations, and limits, see "Resource Allocation Shares," on page 96, "Resource Allocation Reservation," on page 97, and "Resource Allocation Limit," on page 97.

Prerequisites

A reservation pool virtual datacenter.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Properties**.

4   Click the **Resource Allocation** tab and set the priority, reservation, and limit for CPU and memory.

5   Click **OK**.

Modifying Virtual Machine Hard Disks

You can add hard disks, edit hard disks, and delete hard disk from a virtual machine.

You do not have to power off virtual machines that are not fast provisioned to add or edit a virtual machine hard disk.

Add a Virtual Machine Hard Disk

You can add a virtual hard disk to a virtual machine.

Prerequisites

If the virtual machine uses fast provisioning, power off the virtual machine. Non-fast-provisioned virtual machines support adding virtual machine hard disks while the virtual machine is running.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Properties**.

4   Click the **Hardware** tab and click **Add** in the Hard Disks section.

5   Select the disk size, bus type, bus number, and unit number and click **OK**.

6   (Optional) Choose a storage policy for the hard disk.

By default, all the hard disks attached to a virtual machine use the storage policy specified for the virtual machine. You can override this default for any of these disks when you create a virtual machine or modify its properties. The **Size** field for each hard disk includes a drop-down menu that lists all the storage policies available to this virtual machine.

IMPORTANT   You cannot override the default storage policy for any hard disk of a virtual machine that is deployed in a VDC where fast provisioning is enabled.

If the storage policy supports IOPS allocation, a **Disk IOPS** field is displayed. You can accept the default value shown in this field or specify a desired level of disk I/O performance in the range 200-4000. For more information about IOPS, see the *vCloud Director Administrator's Guide*.

What to do next

Use the guest operating system tools to partition and format the new disk.

Change a Virtual Machine Hard Disk

You can change the bus number and unit number of a virtual machine hard disk.

Prerequisites

If the virtual machine uses fast provisioning, power off the virtual machine. Non-fast-provisioned virtual machines support editing virtual machine hard disks while the virtual machine is running.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Properties**.

4 On the **Hardware** tab, select a new size, bus number, and unit number in the Hard Disks section and click **OK**.

Delete a Virtual Machine Hard Disk

You can delete a virtual machine hard disk.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Properties**.

4 Click the **Hardware** tab, click **Delete** in the Hard Disks section, and click **Yes**.

5 Click **OK**.

Modifying Virtual Machine Network Interfaces

You can modify virtual machine network settings, reset a MAC address, add a network interface, and delete a network interface.

Virtual machine version 4 supports up to four NICs, and virtual machine versions 7, 8, 9, and 10 support up to ten NICs. vCloud Director supports modifying virtual machine NICs while the virtual machine is running.

Change Network Interface Settings

You can disconnect a virtual machine NIC, change the network to which a NIC connects, select a primary NIC, and change the IP addressing mode for a NIC.

You do not need to power off the virtual machine to edit network interface settings.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Properties**.

4 Click the **Hardware** tab, and in the NICs section, select the network settings for each NIC.

Option	Action
Connected	Deselect the check box to disconnect a NIC.
Network	Select a network from the drop-down menu.
Primary NIC	Select a primary NIC. The primary NIC setting determines the default and only gateway for the virtual machine. The virtual machine can use any NIC to connect to virtual and physical machines that are directly connected to the same network as the NIC, but it can only use the primary NIC to connect to machines on networks that require a gateway connection.

Option	Action
IP Mode	Select an IP mode.
	■ **Static - IP Pool** pulls IP addresses from the network's IP pool.
	■ **Static - Manual** allows you to specify an IP address.
	■ **DHCP** pulls IP addresses from a DHCP server.
IP Address	If you selected **Static - Manual**, type an IP address.

5   Click **OK**.

Reset a Network Interface MAC Address

You can reset a network interface MAC address if, for example, you have a MAC address conflict or to discard a saved state quickly.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Properties**.

4   Click the **Hardware** tab and in the **NICs** section, select **Reset** from the **MAC Address** drop-down menu..

5   Click **OK**.

Add a Network Interface

You can add one or more virtual NICs to a virtual machine.

Virtual machine version 4 supports up to four NICs, and virtual machine versions 7, 8, 9, and 10 support up to ten NICs. You do not need to power off the virtual machine to add a network interface.

For information about supported network adapter types, see http://kb.vmware.com/kb/1001805.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Properties**.

4   Click the **Hardware** tab, and in the NICs section, click **Add**.

5   (Optional) Modify the NIC settings.

6   Click **OK**.

Remove a Network Interface

You can remove NICs from a virtual machine.

You cannot remove the primary NIC if it is connected to a VCDNI-backed network. If you reconfigure a virtual machine's primary NIC to connect it to a different network, the virtual machine will lose network connectivity if the new network has a different IP configuration (subnet, netmask, gateway, etc.). To restore network connectivity, open the virtual machine console and change the network settings.

You do not need to power off the virtual machine to remove a network interface.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Properties**.

4   Click the **Hardware** tab, and click **Delete** in the NICs section.

5   Click **OK**.

Installing VMware Tools

VMware Tools supports shared folders and cut and paste operations between the guest operating system and the machine from which you launch the vCloud Director Web console.

vCloud Director depends on VMware Tools to customize the guest OS. Using VMware Tools, you can move the pointer in and out of the virtual machine console window.

A virtual machine must be powered on to install VMware Tools.

Install VMware Tools in a New Virtual Machine with No Guest Operating System

If your newly created virtual machine has no guest operating system, you must install it before you can install VMware Tools.

Prerequisites

■   This operation requires the rights included in the predefined vApp User role or an equivalent set of rights.

■   You must have created a vApp that includes a blank virtual machine.

Procedure

1   Click **My Cloud**.

2   In the left pane, select**vApps > Open**.

3   On the **Virtual Machines** tab, select a virtual machine, right-click, and select **Power On**.

4   Log into the virtual machine console and install the guest operating system.

5   Install **VMware Tools**.

6   Power off the virtual machine.

7   Select the virtual machine, right-click and select **Properties**.

8   On the **Guest OS Customization** tab, select the **Enable guest customization** check box.

9   Power the virtual machine on.

The guest OS in your newly created virtual machine has been customized.

Installing VMware Tools in a vApp

When you install VMware Tools in a virtual machine in a vApp, you need to understand the process.

You can trigger VMware Tools installation on a powered on guest virtual machine in a vApp by selecting the virtual machine, right-click, and selecting **Install VMware Tools**. Popout the virtual machine console to continue with the installation. For information on installing in a variety of guest OSs, see Table 8-3.

Table 8-3. Installing VMware Tools

Action	Reference
To install on a Windows Guest	"Install VMware Tools on a Windows Guest," on page 108
To install on a Linux Guest	■ "Use X Windows and RPM to Install VMware Tools on a Linux Guest," on page 109 ■ "Use tar or RPM to Install VMware Tools on a Linux Guest," on page 109
To install on a Solaris Guest	"Install VMware Tools on a Solaris Guest," on page 110

If the settings on a guest virtual machine are not in synch with vCloud Director or an attempt to perform guest customization has failed, you can select the virtual machine, right-click, and select **Power on and Force re-customization**.

When you select **Add to My Cloud** or **Add from Catalog** on a vApp template, these are the available options on the vApp template **Properties** page.

- **Make identical copy**

- **Customize VM Settings**

The vApp template is added and saved as a vApp in your organization. These options are not used when you use a virtual machine, when you create a new vApp, or add a new virtual machine.

Install VMware Tools in a Virtual Machine in a vApp

vApp deployment can fail if VMware Tools are not installed on the virtual machines in the vApp.

Prerequisites

You must stop the vApp.

Procedure

1   Disable Guest Customization on page 102

    To install VMware Tools in a virtual machine in a vApp, you must disable guest customization.

2   Start the vApp on page 103

    After you install VMware Tools, you must start the vApp.

3   Install VMware Tools on page 103

    You must install VMware Tools in your virtual machines to customize the guest operation system.

4   Stop the vApp on page 103

    To enable guest customization on a virtual machine, you must stop the vApp.

5   Enable Guest Customization on page 104

    After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

6   Start the vApp on page 104

    After you install VMware Tools, you must start the vApp.

Disable Guest Customization

To install VMware Tools in a virtual machine in a vApp, you must disable guest customization.

Procedure

1   Click **My Cloud**.

2   In the left pane, select **VMs**.

3   Select a virtual machine, right-click, and select **Properties**.

4   On the **Guest OS Customization** tab, deselect the **Enable guest customization** check box.

Start the vApp

After you install VMware Tools, you must start the vApp.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

     The virtual machines in the vApp will customize when you power on. The guest OS will be rebooted during customization if necessary.

3   Select the vApp, right click, and select **Start**.

Install VMware Tools

You must install VMware Tools in your virtual machines to customize the guest operation system.

Prerequisites

■   This operation requires the rights included in the predefined vApp User role or an equivalent set of rights.

■   Disable guest customization on the relevant virtual machines.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   On the **Virtual Machines** tab, select a virtual machine, right-click, and select **Power On**.

5   Select the virtual machine, right-click, and select **Install VMware Tools**.

     VMware tools installation is triggered or Tools CD is mounted. You need to open the virtual machine console to complete the installation.

VMware Tools is installed.

Stop the vApp

To enable guest customization on a virtual machine, you must stop the vApp.

Prerequisites

This operation requires the rights included in the predefined vApp User role or an equivalent set of rights.

Procedure

1   Click **My Cloud**.

2   Power off your virtual machines.

3   Select a vApp, right-click, and select **Stop**.

The vApp is stopped.

Enable Guest Customization

After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

Procedure

1 On the **Guest OS Customization** tab, select the **Enable guest customization** check box.

2 Select the other check boxes in the dialog box as relevant.

Start the vApp

After you install VMware Tools, you must start the vApp.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **vApps**.

The virtual machines in the vApp will customize when you power on. The guest OS will be rebooted during customization if necessary.

3 Select the vApp, right click, and select **Start**.

Install VMware Tools in a vApp Template

You can install VMware Tools on a virtual machine for which guest customization is enabled.

Prerequisites

Guest customization is enabled on the virtual machine's **Properties** page.

Procedure

1 Save the vApp Template as a vApp on page 104

To install VMware Tools in a vApp, you must save it as a vApp.

2 Disable Guest Customization on page 105

Before you can install VMware Tools on a virtual machine, you must disable guest customization.

3 Install VMware Tools on page 105

You must install VMware Tools in your virtual machines to customize the guest operation system.

4 Enable Guest Customization on page 105

After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

5 Add a vApp to a Catalog on page 106

After you install or upgrade VMware Tools, you can add the updated vApp to your catalog.

Save the vApp Template as a vApp

To install VMware Tools in a vApp, you must save it as a vApp.

Procedure

1 Click **Catalogs**.

2 On the **vApp Templates** tab, select a vApp template, right-click, and select **Properties**.

3 Select **Make Identical Copy**.

4   Select the vApp template, right-click, and select **Add to My Cloud**.

The vApp template has been saved as a vApp.

What to do next

You need to install VMware Tools.

Disable Guest Customization

Before you can install VMware Tools on a virtual machine, you must disable guest customization.

Procedure

1   On the **vApps** page, select a vApp, right-click, and select **Open**.

2   Select **My Cloud** > **vApps**.

3   In a vApp, select a virtual machine, right-click, and select **Open**.

4   On the **Guest OS Customization** tab, deselect the **Enable guest customization** and other check boxes as desired.

5   Select a virtual machine, right-click, and select **Properties**

6   On the **Guest OS Customization** tab, deselect the **Enable guest customization** check box.

7   Select the vApp, right-click, and select **Start**.

Install VMware Tools

You must install VMware Tools in your virtual machines to customize the guest operation system.

Prerequisites

■   This operation requires the rights included in the predefined vApp User role or an equivalent set of rights.

■   Disable guest customization on the relevant virtual machines.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApps**.

3   Select a vApp, right-click, and select **Open**.

4   On the **Virtual Machines** tab, select a virtual machine, right-click, and select **Power On**.

5   Select the virtual machine, right-click, and select **Install VMware Tools**.

     VMware tools installation is triggered or Tools CD is mounted. You need to open the virtual machine console to complete the installation.

VMware Tools is installed.

Enable Guest Customization

After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

Procedure

1   On the **Guest OS Customization** tab, select the **Enable guest customization** check box.

2   Select the other check boxes in the dialog box as relevant.

Add a vApp to a Catalog

After you install or upgrade VMware Tools, you can add the updated vApp to your catalog.

You do not need to stop the vApp before you add it to a catalog. If you add a running vApp to a catalog, the memory state of running virtual machines is preserved and the added vApp is enabled for network fencing.

Procedure

1   Select the vApp, right-click, and select **Add vApp to Catalog**.

2   Select the vApp template, right-click, and select **Properties**.

3   Select **Customize VM Settings** or **Make Identical Copy**.

4   (Optional) Delete any previous versions of the vApp template.

Install VMware Tools With Guest Customization Disabled

You can install VMware Tools in a vApp template when guest customization is disabled.

Prerequisites

Guest customization is disabled on the virtual machine **Properties** page.

Procedure

1   Save the vApp Template as a vApp on page 106

     To install VMware Tools in a vApp, you must save it as a vApp.

2   Install or Upgrade VMware Tools on page 107

     You can either install VMware Tools or upgrade the current version in your virtual machine.

3   Enable Guest Customization on page 107

     After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

4   Add a vApp to a Catalog on page 107

     After you install or upgrade VMware Tools, you can add the updated vApp to your catalog.

Save the vApp Template as a vApp

To install VMware Tools in a vApp, you must save it as a vApp.

Procedure

1   Click **Catalogs**.

2   On the **vApp Templates** tab, select a vApp template, right-click, and select **Properties**.

3   Select **Make Identical Copy**.

4   Select the vApp template, right-click, and select **Add to My Cloud**.

The vApp template has been saved as a vApp.

What to do next

You need to install VMware Tools.

Install or Upgrade VMware Tools

You can either install VMware Tools or upgrade the current version in your virtual machine.

Procedure

1 Click **My Cloud**.

2 In the left pane, select **vApps**.

3 On the **vApps** page, select a vApp, right-click, and select **Open**.

4 Select a virtual machine, right-click, and select **Properties**.

5 In the **Guest OS Customization** tab, deselect the **Enable guest customization** and other check boxes as desired.

6 Right-click the virtual machine and select **Install VMware Tools**.

Enable Guest Customization

After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

Procedure

1 On the **Guest OS Customization** tab, select the **Enable guest customization** check box.

2 Select the other check boxes in the dialog box as relevant.

Add a vApp to a Catalog

After you install or upgrade VMware Tools, you can add the updated vApp to your catalog.

You do not need to stop the vApp before you add it to a catalog. If you add a running vApp to a catalog, the memory state of running virtual machines is preserved and the added vApp is enabled for network fencing.

Procedure

1 Select the vApp, right-click, and select **Add vApp to Catalog**.

2 Select the vApp template, right-click, and select **Properties**.

3 Select **Customize VM Settings** or **Make Identical Copy**.

4 (Optional) Delete any previous versions of the vApp template.

Upgrade VMware Tools

If the version of VMware Tools is earlier than 7299 in a virtual machine in your vApp, you must upgrade it.

Upgrading VMware Tools might involve uninstalling your existing VMware Tools versions and installing a new one from a CD mounted in the operating system. This process can also be done automatically.

Prerequisites

You must stop the vApp.

Procedure

1 Install a New Version of VMware Tools on page 108

   After you disable guest customization, you can upgrade VMware Tools.

2 Enable Guest Customization on page 108

   After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

3

    After you install VMware Tools, you must start the vApp.

Install a New Version of VMware Tools

After you disable guest customization, you can upgrade VMware Tools.

Procedure

1 Select the vApp, right-click, and select **Start**.

2 Select the virtual machine, right-click, and select **Install VMware Tools**.

    The process is different based on the operating system.

Enable Guest Customization

After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

Procedure

1 On the **Guest OS Customization** tab, select the **Enable guest customization** check box.

2 Select the other check boxes in the dialog box as relevant.

Start the vApp

After you install VMware Tools, you must start the vApp.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **vApps**.

    The virtual machines in the vApp will customize when you power on. The guest OS will be rebooted during customization if necessary.

3 Select the vApp, right click, and select **Start**.

Install VMware Tools on a Windows Guest

vCloud Director uses VMware Tools to customize the Windows guest operating system.

Prerequisites

■ The VMware Remote Console application is installed.

■ Your virtual machine is powered off.

■ You have disabled the option to install VMware Tools on a powered off virtual machine.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a virtual machine, right-click, and select **Install VMware Tools**.

4 Follow the prompts to complete the installation wizard.

5 Click **Finish**.

6 Restart your virtual machine.

Use X Windows and RPM to Install VMware Tools on a Linux Guest

You can use X Windows to access a VM and run an RPM installer to install VMware Tools on a Linux guest operating system.

Prerequisites

The VMware Remote Console application installed.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a Linux virtual machine, right-click, and select **Popout Console**.

4   In the guest operating system, start the RPM installer.

- Double-click the VMware Tools CD icon on your desktop and double-click the RPM installer in the root of the CD-ROM.

- Double-click the RPM installer in the file manager window.

5   Type the root password and click **OK**.

6   Click **Continue** when the package is ready.

After VMware Tools is installed, no confirmation appears.

7   In an X terminal, as root, run the `vmware-config-tools.pl` script to configure VMware Tools.

8   Press Enter to accept the default value.

9   After the upgrade is complete, enter **/etc/init.d/network** to restart the network.

10 Type **exit**.

11 To start the VMware Tools control panel, enter **vmware-toolbox &**.

Use tar or RPM to Install VMware Tools on a Linux Guest

You can use the Linux tar or RPM utilities to install VMware tools on a Linux guest OS.

Prerequisites

- The VMware Remote Console application installed.

- The virtual machine is powered on.

- With an existing installation, delete the **vmware-tools-distrib** directory before you install. The location of this directory depends on where you placed it during the previous installation (such as, **tmp/vmware-tools-distrib**).

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a Linux virtual machine, right-click, and select **Install VMware Tools**.

4   Right-click the virtual machine again and click **Popout Console**.

5 In the guest operating system, log in as root (su–), mount the VMware Tools virtual CD-ROM image, and change to a working directory (for example, **/tmp**.

Some Linux distributions automatically mount CD-ROMs. If your distribution uses automounting, do not use the mount and unmount commands. You still must untar the VMware Tools installer to /tmp. Some Linux distributions use different device names or organize the /dev directory differently. If your CD-ROM drive is not /dev/cdrom, or if the mount point for a CD-ROM is not /mnt/cdrom, modify these commands to reflect the conventions used by your distribution.

```
mount /dev/cdrom /mnt/cdrom
cd /tmp
```

6 Uncompress the installer and unmount the CD-ROM image.

If you install an RPM installation over a tar installation, or the reverse, the installer detects the previous installation and must convert the installer database format before continuing.

Option	Action
In the tar installer	At the command prompt, type **tar zxpf /mnt/cdrom/VMwareTools–n.n.n–xxxxxx.tar.gz unmount /dev/cdrom** where *n.n.n* is the VMware Tools version and *xxxxxx* is the build or revision number of the release.
In the RPM installer	At the command prompt, type **tar zxpf /mnt/cdrom/VMwareTools–n.n.n–xxxxxx.i386.gz unmount /dev/cdrom** where *n.n.n* is the VMware Tools version and *xxxxxx* is the build or revision number of the release.

7 Run the installer.

Option	Action
In the tar installer	Type **cd vmware–tools–distrib./vmware–install.pl**. Press Enter to accept the default values.
In the RPM installer	Configure VMware Tools, type **vmware–config–tools.pl** Press Enter to accept the default values.

8 After the upgrade is complete, restart the network by running **/etc/init.d/network restart**.

9 Type **exit**.

10 Start your graphical environment.

11 In an X terminal, run **vmware–toolbox &**.

Install VMware Tools on a Solaris Guest

You can install VMware Tools on a Solaris guest OS.

Prerequisites

The VMware Remote Console application is installed.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Select a Solaris virtual machine, right click, and select **Install VMware Tools**.

4 Click **Popout Console**.

5   In the virtual machine, log in as root and, if necessary, mount the VMware Tools virtual CD-ROM image.

    The Solaris volume manager vold mounts the CD-ROM under `/cdrom/vmwaretools`.

6   If the CD-ROM is not mounted, restart the volume manager by running these commands.

    ■   `/etc/init.d/volmgt stop`

    ■   `/etc/init.d/volmgt start`

7   After the CD-ROM is mounted, change to a working directory, for example, `/tmp` and extract VMware Tools.

    ■   `cd /tmp`

    ■   `gunzip -c /cdrom/vmwaretools/vmware-solaris-tools.tar.gz | tar xf -`

8   Run the VMware Tools tar installer.

    ■   `cd vmware-tools-distrib`

    ■   `./vmware-install.pl`

9   Press Enter to accept the default value.

10 Type `exit`.

11 Start your graphical environment.

12 In an X terminal, enter `vmware-toolbox &`.

Guest Operating Systems

A guest operating system is an operating system that runs inside a virtual machine. You can install a guest operating system in a virtual machine and control guest operating system customization for virtual machines created from vApp templates.

In "Guest Operating System Support," on page 116, you can see a list of the supported guest operating systems and whether customization is automatic or manual.

Install a Guest Operating System

With a guest OS you can manage virtual machines that are based on the available operating systems.

Prerequisites

The appropriate media file must be in your catalog.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Insert CD/DVD**.

4   Select an available media file in the top panel or select one and add it to your virtual datacenter in the bottom panel.

5   Click **OK**.

6   Point to the virtual machine name and press Ctrl+Alt+Del to boot from the ISO image and start the operating system installer.

7   In the virtual machine console, type the required information to complete the installation.

8   Click **Finish**.

Customizing Your Guest Operating System

When you customize your guest OS you can set up a virtual machine with the operating system that you want.

vCloud Director can customize the network settings of the guest operating system of a virtual machine created from a vApp template. When you customize your guest operating system, you can create and deploy multiple unique virtual machines based on the same vApp template without machine name or network conflicts.

When you configure a vApp template with the prerequisites for guest customization and add a virtual machine to a vApp based on that template, vCloud Director creates a package with guest customization tools. When you deploy and power on the virtual machine for the first time, vCloud Director copies the package, runs the tools, and deletes the package from the virtual machine.

Understanding Guest Customization

When you customize your guest operating system, there are some settings and options you should know about.

Enable Guest Customization Check Box

This check box is found on the **Guest OS customization** tab on the virtual machine **Properties** page. The goal of guest customization is to configure based on the options selected in the **Properties** page. If this check box is selected, guest customization and re-customization is performed when required.

This process is required for all guest customization features, such as the computer name, network settings, setting and expiring the administrator/root password, SID change for Windows Operating systems, and so on, to work. This option should be selected for **Power on and Force re-customization** to work.

If the check box is selected, and the virtual machine's configuration parameters in vCloud Director are out of synch with the settings in the guest OS, the **Profile** tab on the virtual machines **Properties** page displays that the settings out of synch with the guest OS and the virtual machine needs guest customization.

Guest customization Behavior for vApps and Virtual Machines

The check boxes are deselected.

- **Enable guest customization**
- In Windows guest OSs, **Change SID**
- **Password reset**

If you want to perform customization (or you made changes to network settings that need to be reflected in the guest OS), you can select the **Enable guest customization** check box and set the options on the **Guest OS Customization** tab of the virtual machine **Properties** page. When virtual machines from vApp templates are used to create a new vApp and then add a virtual machine, the vApp templates act as building blocks. When you add virtual machines from the catalog to a new vApp, the virtual machines are enabled for guest customization by default. When you save a vApp template from a catalog as a vApp, virtual machines are enabled for guest customization only if the **Enable guest customization** check box is selected.

These are the default values of guest customization settings:

- The **Enable guest customization** check box is the same as the source virtual machine in your Catalog.
- For Windows guest virtual machines, **Change SID** is the same as the source virtual machine in your catalog.
- The password reset setting is same as the source virtual machine in your catalog.

You can deselect the **Enable guest customization** check box if required before you start the VApp.

If blank virtual machines, which are pending guest OS installation, are added to a vApp, the **Enable guest customization** check box is deselected by default because these virtual machines are not yet ready for customization .

After you install the guest OS and VMware Tools, you can power off the virtual machines, stop vApp, and select the **Enable guest customization** check box and start the vApp and virtual machines to perform guest customization.

If the virtual machine name and network settings are updated on a virtual machine that has been customized, the next time you power on the virtual machine, it is re-customized, which resynchronizes the guest virtual machine with vCloud Director

Customizing a Guest OS When Saving a vApp Template as a vApp

Before you customize a guest OS in a vApp template, you need to understand the settings you need to make.

On the **vApp Templates Properties** page, if you select **Customize VM Settings** for the **When creating a vApp from this template** option, and you select **Add to My Cloud** or **Add from Catalog**, the **Enable guest customization** check box is selected by default and guest customization is performed.

These are the default values of guest customization settings.

- The **Enable guest customization** check box is selected.

- For Windows guest VMs, the **Change SID** option is the same as the source virtual machine in your catalog.

- Password reset setting is the same as the source virtual machine in your catalog.

If you select **Make Identical Copy** on the vApp template **Properties** page, and select **Add to My Cloud**, the settings in the vApp Template are applied to the new vApp, regardless of whether customization is enabled.

These are the default values of guest customization settings.

- The **Enable guest customization** check box is deselected.

- In Windows guest virtual machines, the **Change SID** check box is deselected.

- The password reset setting is deselected.

After you import or upload to a catalog, these are the default values.

- The **Customize VM Settings** check box is selected in the vApp

- The **Enable guest customization** check box is selected for the virtual machines.

- For Windows guest VMs, the **Change SID** check box is selected for the virtual machines.

- The Password reset setting is selected by default for the virtual machines.

If you are a vApp template owner and you import or upload to a catalog, you must check the VMware Tools version installed on the virtual machines in the vApp. To do this, select the vApp template, right-click, and select **Open**. Tools version is shown in the **VMware Tools** column. If you select **Customize VM Settings**, VMware Tools should be installed on all virtual machines. See "Installing VMware Tools," on page 101 for more information.

Enable or Disable Guest Customization

You can disable guest customization for a virtual machine or a vApp template.

Prerequisites

VMware Tools is installed.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **vApp** or **VMs**.

3   Select a vApp or virtual machine, right-click, and select **Properties**.

4   On the **Guest OS Customization** tab, select or deselect the **Enable guest customization** check box.

5   Click **OK**.

Guest customization in the selected virtual machine is enabled or disabled.

Change Guest Customization Settings for Virtual Machines in a vApp Template

You can change the guest customize settings on virtual machines in a vApp template when the virtual machines are used as building blocks to create a new vApp.

Procedure

1   Click **Catalogs**.

2   On the **vApp Templates** tab, select a vApp template, right-click, and select **Add to My Cloud**.

The vApp template is saved as a vApp.

3   Select the vApp, right-click, and select **Open**.

4   On the **Virtual Machines** tab, select the virtual machine, right-click, and select **Properties**.

5   On the **Guest Customization OS** tab, select or deselect the **Enable guest customization** check box and click **OK**.

6   Select the vApp, right-click, and select **Add to Catalog**.

The vApp is saved as a vApp template in the selected catalog.

Power on and Force Recustomization of a Virtual Machine

If the settings on a guest virtual machine are not in synch with vCloud Director or an attempt to perform guest customization has failed, you can power on and force the recustomization of the virtual machine.

Prerequisites

This operation requires the rights included in the predefined vApp User role or an equivalent set of rights.

Procedure

1   Click **My Cloud**.

2   In **vApps**, select a vApp, right-click, and select **Open**.

3   On the **Virtual Machines** tab, select a virtual machine, right-click, and select **Power On and Force Re-customization**.

NOTE   If you select the **Change SID** check box, the Windows machine Security Identifier (machine SID) of the guest OS is changed during guest customization.

The virtual machine is now recustomized.

Upload a Customization Script

You can upload a customization script to a virtual machine. The script runs before and after guest customization when you deploy a virtual machine based on a vApp template.

When you add a customization script to a virtual machine, the script is called:

■ Only on initial customization and force recustomization.

■ With the "precustomization" command line parameter before guest customization begins.

■ With the "postcustomization" command line parameter after guest customization finishes.

The customization script cannot exceed 1500 characters.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 In the right pane, select a virtual machine, right-click, and select **Properties**.

4 On the **Guest OS Customization** tab, in the **Customization Script** panel, click **Browse**.

5 Navigate to your script file and click **Open**.

The file must be a batch file for Windows virtual machines and a shell script for Unix virtual machines.

6 Click **OK**.

Example: Customization Script Examples

A sample Windows batch file:

```
 @echo off
if "%1%" == "precustomization" (
echo Do precustomization tasks
) else if "%1%" == "postcustomization" (
echo Do postcustomization tasks
)
```

A sample Unix shell script:

```
 #!/bin/sh
if [ x$1 == x"precustomization" ]; then
echo Do Precustomization tasks
elif [ x$1 == x"postcustomization" ]; then
echo Do Postcustomization tasks
fi
```

Reset Your Virtual Machine's Password

You can reset your virtual machine's password.

Prerequisites

The virtual machine's guest OS is personalized, and your virtual machine is powered off.

Procedure

1 Click **My Cloud**.

2 In the left pane, click **VMs**.

3 Right-click a virtual machine and select **Properties**.

4   On the **Guest OS Customization** tab, select the **Enable guest customization** check box.

5   Select **Allow local administrator password**.

6   Select **Require administrator to change password on first login** to require all administrators to change the password upon initial log in.

Administrators must know the old password.

7   Choose how to generate the virtual machine password.

Option	Description
Auto generate password	vCloud Director generates a password for the virtual machine.
Specify password	Type a password for the virtual machine.

8   (Optional) Select **Automatically log on as Administrator** for vCloud Director to log on as Administrator when the virtual machine powers on and select the number of times to log on automatically from the drop-down list.

9   Click **OK**.

The password for your virtual machine is reset.

Join a Windows Guest Domain During Guest Operating System Personalization

A virtual machine can join a Windows guest domain when you personalize your guest OS.

Prerequisites

On a virtual machine's **Properties** page, verify that the **Enable guest customization** check box is selected.

Procedure

1   Click **My Cloud**.

2   In the left pane, click **VMs**.

3   Select a virtual machine, right-click, and select **Properties**.

4   On the **Guest OS Customization** tab, select the **Enable this VM to join a domain** check box.

Override organization settings is selected by default.

5   Type a domain name, user name, password, and account organizational unit.

6   Under **Customization Script**, click **Browse**, to upload a locally saved file.

7   Click **OK**.

The selected virtual machine joins the Windows guest domain.

Guest Operating System Support

vCloud Director supports a wide variety of 32-bit and 64-bit operating systems in its virtual machine templates and virtual machines.

See the *vCloud Director Release Notes* for a list of guest operating systems supported by this release of vCloud Director.

Index