manx telecom

Intelligent cloud

User Guide

vmware®

Table of Contents

1 Getting Started with Intelligent Cloud

When you log in to the Intelligent Cloud Web portal, 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:

- 1.1 Understanding the platform
- 1.2 Logging into the Web Portal
- 1.3 Using the portal
- 1.4 Set Mozilla Firefox options
- 1.5 Set Microsoft Internet Explorer options
- 1.6 Set User preferences
- 1.7 Change your password

1.1 Understanding the platform

The Intelligent Cloud platform provides role-based access to a Web portal that allows the members of an organisation to interact with that organisation's resources to create and work with vApps and virtual machines. Before you can access your organisation, Manx Telecom will provision and Organisation, assign it resources, and provide the URL to access the Web console. This URL will look like:

https://www.thecloud.im/cloud/org/orgname

Each organisation includes one organisation administrators, who can then finishes setting up the organisation by adding additional members and setting policies and preferences. After the organisation is set up, non-administrator users can log in to create, use, and manage virtual machines and vApps.

1.1.1 Organisations

An organisation is a unit of administration for a collection of users, groups, and computing resources. Users authenticate at the organisation level, supplying their credentials configured by the default organisation administrator when the user was created. Manx Telecom creates and provision organisations, while organisation administrators manage organisation users, groups, and that organisations catalogs.

1.1.2 Users and Groups

An organisation can contain an arbitrary number of users and groups. Users can be created locally by the organisation administrator. Permissions within an organisation are controlled through the assignment of rights and roles to users and groups.

1.1.3 Virtual Datacenters (or vDC)

An organisation virtual datacenter (vDC) provides resources to an organisation. vDCs provide an environment where virtual systems can be stored, deployed, and operated. They also provide storage for virtual media, such as floppy disks and CD ROMs. An organisation by default will only have one vDC.

1.1.4 Virtual Machines (or VM)

A VM is a virtualised implementation of a common-or-garden computer, equipped with 1 or more vCPUs, some memory, 1 or more disk drives and network connections. It would house a guest operating system such as Windows or Linux, and any application workloads that need to be run within that machine.

1.1.5 vApps

A vApp or 'Virtual Application' is simply a container for one or more virtual machines (see 1.1.4 Virtual Machines). A vApp can have special rules applied to it for the order and timing of contained VMs to be power on or powered off, including their default action (power off / shutdown etc). vApps can be configured with "lease times" which provides the ability to automatically power off or have themselves purged at a specific time (alerts are sent to the organisation administrator warning of lease time based operations). Multiple vApps can be connected to Organisation networks (see 1.1.6 Organisation Networks), and each vApp can have isolated vApp networks added within them (see 1.1.7 vApp Networks).

1.1.6 Organisation vDC Networks

An organisation vDC network is contained within a organisation vDC and is available to all the vApps in that organisation. An organisation vDC network allows vApps within an organisation to communicate with each other. By default one organisation vDC network will be created and this will be used for external access to the Internet. We will supply one or more IP addresses for this network. Organisation administrators can manage organisation networks, including the network services they provide such as NAT, SSL VPN, firewall and load balancer rules.

1.1.7 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 organisation network to allow the vApp to communicate with other vApp networks in the organisation (and outside of the organisation), a vApp network must be routed via an Organisation network (see 1.1.6 Organisation Networks).

1.1.8 Catalogs

Organisations use catalogs to store vApp templates and media files. The members of an organisation that have access to a catalog can use the catalog's vApp templates and media files to create their own vApps. Organisations administrators can copy items from public catlogs to their organisation catalog.

1.2 Logging In to the Web Portal

Use the organisation URL see section 1.1) to log in to your organisation and access the Web console. Contact us if you do not know the organisation URL.

Procedure

1) In a browser, type the URL of your organisation and press Enter. For example, type https://www.thecloud.im/cloud/org/orgname.
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 organisation administrator can click the “Set up this organisation” link on the Home tab to finish setting up a newly created organisation. See “Set Up an Organisation,” on page 38 for more information.

1.3 Using the portal

When you log log into the portal, the first page you see is the Home page. The information that appears on this page are the most common tasks for your role. Organisation administrators see the Set up this organisation link as their first task. They also see tasks under these headings.

- Organisations and resources
- Content
- Users & Groups

The vApps in your organisation 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

Console Access Only users have a read-only access to the portal. (and access to the VM Consoles)

1.4 Set Mozilla Firefox Options

These options and settings help you display and use the Web portal in Mozilla Firefox.

Prerequisites
You have the following

- At least Firefox 3.x
- SSL 3.0 Encryption
- TLS 1.0 Encryption

Procedure
In Firefox, select Tools > Options.

1) Click Content and select the JavaScript check box.
2) Click Privacy.
3) In the Firefox will: drop-down menu, select Use custom settings for history.
4) Select the Accept cookies from sites. This selection also selects the Accept third-party cookies check box.
5) Click OK.

1.4.1 Bypass the Proxy in Mozilla Firefox

You can configure the Firefox proxy server to bypass certain Web addresses.
If all of these conditions exist, you can configure Firefox to bypass specific Web addresses.

- The internal network is configured with a proxy server to access the external network.
- The browser's proxy server connection has no local exceptions.
- The proxy is not configured to look in the internal network after not finding or connecting to the target on the external network.
- The user looks for a target on the internal network using Firefox.

Procedure

1) Select an option

Operating System	**Action**
Windows	Tools - Options
Linux	Edit - Preferences

2) Click the **Advanced** button.
3) On the **Network** tab, click the **Settings** button.
4) Enter the IP of the cell or load balancer in the **No Proxy for:** field.

The specified Web addresses are bypassed by the Firefox proxy server.

1.5 Set Microsoft Internet Explorer Options

These options help you display and use the Web portal in Microsoft Internet Explorer.
You have the following.

- At least Internet Explorer 7.
- SSL 3.0 Encryption
- TLS 1.0 Encryption

Procedure

1) In Internet Explorer, select **Tools > Internet Options**.
2) Click the **Security** tab.
3) Select the **Internet content** zone for the www.thecloud.im server.

4) Click **Custom Level** and select **Enable** or **Prompt** for these options.
   - **Download signed ActiveX controls**
   - **Run ActiveX controls and plug-ins**
   - **Allow META REFRESH**
   - **Active scripting of Microsoft web browser control**
5) Click **OK**.
6) Click the **Advanced** tab.
7) If you are using Internet Explorer on Windows 2003, complete these tasks.
   a. Select **Start > Settings > Control Panel**.
   b. Select **Add or Remove Programs**.
   c. Click **Add/Remove Windows Components**.
   d. Disable **Internet Explorer Enhanced Security Configuration**.

1.5.1 Bypass the Proxy in Internet Explorer

You can configure the Internet Explorer proxy server to bypass certain Web addresses.
If all of these conditions exist, you can configure Internet Explorer to bypass specific Web addresses.

- The internal network is configured with a proxy server to access the external network.
- The browser's proxy server connection has no local exceptions.
- The proxy is not configured to look in the internal network after not finding or connecting to the target on the external network.
- The user looks for a target on the internal network using Internet Explorer.

Procedure

1) Type the IP address of the cell or load balancer so that VMware Remote Console (VMRC) can bypass the proxy setting.
2) Select **Tools > Internet Options**.
3) On the **Connections** tab, click **LAN Settings** in the bottom panel.
4) In the Proxy Server panel, click **Advanced**.
5) In the Exception panel, in the **Do not use proxy server for addresses beginning with:** text box, type in the IP address 80.65.255.6 (the IP address of the Intelligent Cloud Web Portal). If the configuration management vehicle supports the use of regular expressions, you must type the DNS name e.g. www.thecloud.im
6) Click **OK**.

The specified Web addresses are bypassed by the Internet Explorer proxy server.

1.6 Set User Preferences

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

Procedure

1) In the title bar of the Web console, click **Preferences**.
2) Click the **Defaults** tab.
3) Select the page to display when you log in.
4) Select the number of days or hours before a runtime lease expires that you want to receive an email notification.
5) Select the number of days or hours before a storage lease expires that you want to receive an email notification.
6) Click **OK**.

1.7 Change Your Password

You can change your password.

Procedure

1) Log in to your organisation.
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**.

The platform will log you out.

What to do next

Log in using your new password.

2 Managing Users

An organisation administrator is the only one who can add users and groups to an organisation. The organisation administrator assigns each user or group a role within the organisation. Your role controls what you can see and do in the Intelligent Cloud portal. An organisation administrator can create local user accounts within an organisation which can have one of the default roles:

Organisation Administrator	Administers the organisation
Catalog Author	Creates and publishes new catalogs
vApp Author	Creates vApps and uses catalogs
vApp User	Uses vApps created by others
Console Access Only	Uses VM guest OS and views VM state and properties

This chapter includes the following topics:

- 2.1 Managing Users

2.1 Managing Users

The **Users** page displays a list of users your organisation. You can see whether the users are active and their role. As an organisation administrator, you can complete these operations.

- Add a new user
- Send email notifications
- Deactivate a user
- Modify a user's properties
- Delete a user

2.1.1 Add a User

Adding local users allows organisation administrators to provide access to users

Procedure

1) Click **Administration**.
2) In the left pane, select **Members > Users**.
3) Click the **New User** button.
4) Type the user name and password.
5) Select a role.
6) (Optional) Type the contact information.
7) Select the stored and running virtual machine quota limits for this user.
8) Click **OK**.

The new user appears on the **Users** page.

2.1.2 Edit a User

An organisation administrator can edit local user properties such as the password, role, contact information and quotas.

Procedure

1) Click **Administration**.
2) In the left pane, select **Members > Users**.
3) Select a user, right-click, and click **Properties**.
4) Modify the necessary properties and click **OK**.

2.1.3 Delete a User

If a user leaves the organisation, an organisation administrator can delete a user from the organisation.

Procedure

1) Click **Administration**.
2) In the left pane, select **Members > Users**
3) Select a user, right-click, and select **Disable Account**.
4) Reselect this user, right-click, and select **Delete**.
5) Click **OK**.

The user is deleted from your organisation.

2.1.4 Send User Notifications

An organisation administrator can send an email notification to users to notify them of events or issues in the organisation.

Procedure

1) Click **Administration**.
2) In the left pane, select **Members > Users**. Click the **Notify** button.

   If you select a user and then click this button, the user's name appears as the recipient.

3) Select the recipients and type a subject.
4) Type the message.
5) Click **Send Email**.

The notification is sent to the selected recipients.

2.1.5 Disable or Enable User Accounts

An organisation administrator can disable a user account to log the user out of the Web console and prevent the user from logging in again. You can enable a user to allow them to log in.

Procedure

1) Click **Administration**.
2) In the left pane, select **Members > Users**.
3) Select a user, right-click, and select **Disable Account** or **Enable Account**.

Disabled user accounts have a red circle in the **Enabled** column and enabled user accounts have a green check mark.

What to do next

After you disable a user's account, you can delete that user. See Delete a User in section 2.4.

2.1.6 View and Change a User's Role

An organisation administrator assigns a role when adding a user to the organisation. The organisation administrator can change the user's role later to give the user more rights or fewer rights.

Procedure

1) Click **Administration**.
2) In the left pane, select **Members > Users**.
3) Select a user, right-click, and select **Properties**.
4) In the **User role in organisation:** drop-down menu, select a new role for the user. The definition of each role appears as a tool tip.
5) Click **OK**.

3 Managing Cloud Resources

Manx Telecom will assign a virtual datacenter (vDC) and organisation networks to an organisation. An organisation administrator can view information about these resources and perform a limited set of management tasks.

This chapter includes the following topics:

- 3.1 Managing Virtual Datacenters
- 3.2 Managing Organisation vDC Networks
- 3.3 Managing Expired Items

3.1 Managing Virtual Datacenters

Virtual datacenters (vDCs) provide processor, memory, and storage resources to your organisation. They are assigned to your organisation and only one is provided by default.

3.1.1 Display Virtual Datacenters

When you display the vDC in your organisation, you can monitor the resources, users, and policy settings that you manage.

You are an organisation administrator.

Procedure

1) Click **Administration**.
2) In the left pane, select **Cloud Resources > Virtual Datacenters**.
3) The vDC for your organisation will appear in the right pane.
4) For details about the vDC, right-click, and select **Open**.

The vApps, vApp templates, media, and networks attached to this vDC are displayed. When you click through each tab, you can right click on an object to see the operations you can complete.

3.1.2 Review Virtual Datacenter Properties

You can review the properties of the vDC that is assigned to your organisation.

Procedure

1) Click **Administration**.
2) Select **Cloud Resources > Virtual Datacenters**.
3) Select the vDC, right-click, and select **Properties**.
4) Review the properties and click **OK**.

What to do next

Contact us if you wish to modify your organisational vDC

3.1.3 Monitor Your Virtual Datacenter

You can monitor the vDC assigned to your organisation and determine when to request additional capacity if required.

You are an organisation administrator.

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 us is more capacity is required.

3.1.4 Manage Your Virtual Datacenters

You can review information such as the status, allocation model, and the number of vApps in a vDC in your organisation. You are an organisation administrator.

Procedure

1) Click **Administration**.
2) In the left pane, select **Cloud Resources > Virtual Datacenters.**
3) Click the **Manage** button.
4) Review the information.

What to do next

You can open the vDC to see the objects in it, notify users about issues or changes, or review the vDC’s properties. Contact us to make changes to your vDC.

3.2 Managing Organisation vDC Networks

Organisation networks are created and assigned to your organisation by us. An organisation administrator can view information about these networks, configure network services, and more. There are three type of organisation vDC networks.

Table 3-1. Types of Organisation vDC Networks

Organisation Network Type	Description
Direct	Accessible by multiple organisations. Virtual machines belonging to different organisations can connect to and see traffic on this network. This network provides direct layer 2 connectivity to machines outside of the organisation. Machines outside of this organisation can connect to machines within the organisation directly.
Routed	Accessible only by this organisation. Only virtual machines within this organisation can connect to this network. This network also provides controlled access to an external network. System administrators and organisation 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 organisation. Only virtual machines within this organisation can connect to and see traffic on this network. This network provides an organisation with an isolated, private network that multiple vApps can connect to. This network provides no connectivity to machines outside this organisation. Machines outside of this organisation have no connectivity to machines within the organisation.

By default, the organisation network that is added to a customer vDC will always be of the **routed** type to provide external connectivity to the Internet.

3.2.1 Configuring Network Services for an Organisation Network

An organisation administrator can configure network services, such as DHCP, firewalls, network address translation (NAT), VPN, and static routing for certain organisation vDC networks. The network services available depend on the type of organisation network.

See also

- Aspects of 3.2 Managing Organisation vDC Networks
- Aspects of 8.14 Working with Networks in a vApp
- Review sample network configurations in Appendix A - sample vApp network configurations

Table 3-2. Network Services Available by Network Type

Organisation Network Type	DHCP	Firewall	NAT	VPN	Static Routing
Direct					
Routed	X	X	X	X	X
Internal	X				

3.2.1.1 Configure DHCP for an Organisation vDC Network

Organisation administrators can configure certain organisation networks to provide DHCP services to virtual machines in the organisation. When you enable DHCP for an organisation network, connect a NIC on a virtual machine in the organisation to that network, and select **DHCP** as the IP mode for that NIC, the platform assigns a DHCP IP address to the virtual machine when you power it on.

Prerequisites

- A *routed* organisation vDC network or an internal organisation vDC network.

Procedure

1) Click **Administration** and select the organisation vDC
2) Click the **Org vDC Networks** tab, right click the organisation vDC network name and select **Configure Services**.
3) Select **Enable DHCP**
4) Type a range of IP addresses or use the default range.

   The platform uses these addresses to satisfy DHCP requests. The range of DHCP IP addresses cannot overlap with the static IP pool for the organisation vDC network.

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

The platform will update the network to provide DHCP services.

3.2.1.2 Configure the Firewall for an Organisation vDC Network

An organisation administrator can configure certain organisation networks to provide firewall services. Enable the firewall on an organisation 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 3.2.1.3 Add a Firewall Rule to an Organisation vDC Network

If the syslog vApp is deployed in your cloud, then you can log events related to the default firewall action. For information about adding the syslog vApp to your cloud see 3.2.7 Apply Syslog Server Settings to an Organisation vDC Network.

Prerequisites

- A *routed* organisation network. (see 3.2 Managing Organisation vDC Networks)

Procedure

1) Click **Administration** and select the organisation vDC
2) Click the **Org vDC Networks** tab, right click the organisation vDC network name and select **Configure Services**.
3) Click the **Firewall** tab and select **Enable firewall**.
4) Select the default firewall action.
   Allow – Allow all traffic except when overridden by a deny firewall rule
   Deny – Block all traffic except when overridden by an allow firewall rule
5) (Optional) Select the **Log** check box to log events related to the default firewall action. (requires syslog vApp to be deployed to observe events)
6) Click **OK**.

3.2.1.3 Add a Firewall Rule to an Organisation vDC Network

An organization administrator can add firewall rules to an organization vDC network that supports a firewall. You can create rules to allow or deny traffic that matches the rules to pass through the firewall. When you add a new firewall rule to an organization vDC network, it appears at the bottom of the firewall rule list. For information about how to set the order in which firewall rules are enforced, see 3.2.1.4 Reorder Firewall Rules for an Organization vDC Network.

If a syslog vApp is applied to your organisation then you can log firewall rule events. For information about applying syslog server settings, see 3.2.7 Apply Syslog Server Settings to an Organisation vDC Network To view the current syslog server settings see 3.2.6 View Syslog Server Settings for an Organisation or vApp Network

Prerequisites

- A routed organisation network 3.2 Managing Organisation vDC Networks that has the firewall enabled 3.2.1.2 Configure the Firewall for an Organisation vDC Network

Procedure

1) Click **Administration** and select the organisation vDC
2) On the Org vDC Networks tab, right click the organisation vDC network name and select **Configure Services**
3) Click the **Firewall** tab and click **Add**.
4) Type a name for the rule.
5) (Optional) Select **Match rule on translated IP** to have the rule check against translated addresses rather than original public IP addresses and choose traffic direction to apply the rule on

6) Type the traffic **Source**

Option	Description
IP address	Type a source IP address to apply the rule on (e.g 192.168.0.100)
Range of IP addresses	Type a range of source IP addresses to apply this rule on (e.g. 192.168.0.100 – 192.168.0.150)
CIDR	Type the CIDR notation of traffic to apply this rule on (e.g. 192.168.0.0/24)
Internal	Apply this rule to internal traffic only
External	Apply this rule to external traffic only
Any	Apply this rule to traffic from any source

For incoming traffic, the source is the external network. For outgoing traffic, the source is the organisation vDC network.

7) Select a **Source port** from the drop-down menu
8) Type the traffic **Destination**

Option	Description
IP address	Type a source IP address to apply the rule on (e.g 192.168.0.100)
Range of IP addresses	Type a range of source IP addresses to apply this rule on (e.g. 192.168.0.100 – 192.168.0.150)
CIDR	Type the CIDR notation of traffic to apply this rule on (e.g. 192.168.0.0/24)
Internal	Apply this rule to internal traffic only
External	Apply this rule to external traffic only
Any	Apply this rule to traffic from any source

9) Select the **Destination port** to apply this rule on from the drop-down menu
10) Select the **Protocol** to apply this rule on from the drop-down menu
11) Select the action (A firewall rule can allow or deny traffic that matches a rule)
12) Select the **Enabled** check box
13) (Optional) Select the **Log network traffic for firewall rule** check box.

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

1) Click **OK** and **OK** again.

3.2.1.4 Reorder Firewall Rules for an Organisation vDC Network

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

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

Prerequisites

- A routed organisation vDC network with two of more firewall rules in place

Procedure

1) Click **Administration** and select the organisation vDC
2) Clickd the Org vDC Networks tab, right-click the organisation vDC 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**.

3.2.1.5 Enable VPN for an Organisation vDC Network

An organization administrator can enable VPN for an organization vDC network, then create a secure tunnel to another network. The platform supports VPN between organization vDC networks in the same organization and remote networks.

Prerequisites

- A routed organisation vDC network (see 3.2 Managing Organisation Networks)

Procedure

1) Click **Administration** and select the organisation vDC.
2) Select **Org vDC Networks**, right click the organisation vDC network name and select **Configure Services**
3) Click the **VPN** tab and select **Enable VPN**
4) (Optional) Type a public IP address.
5) Click **OK**

What to do next

Create a VPN tunnel to another network

3.2.1.6 Create a VPN tunnel in an Organisation

An organisation administrator can create a VPN tunnel between two organisations vDC networks in the same organisation. 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

Prerequisites

- At least two routed organisation networks with non-overlapping IP subnets and VPN enabled on both networks

Procedure

1) Click **Administration** and select the organisation vDC.
2) Select **Org vDC Networks**, right click the organisation vDC network name and select **Configure Services**
3) Click the **VPN** tab and select **Add**
4) Type a name and optional description.
5) Select **a network in this organisation** from the drop-down menu and select a peer network.
6) Review the tunnel settings and click **OK**.

The platform will configure both peer network endpoints.

3.2.1.7 Create a VPN Tunnel Between Organisations

An organisation administrator can create a VPN tunnel between two organisation vDC networks in different Organisations. The organisations can be part of the Intelligent Cloud or a different **VMware vCloud Director** driven cloud installation elsewhere. 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

Prerequisites

- A routed organisation vDC network in each of the organisations.
- The organisation networks must have non-overlapping IP subnets and site-to-site VPN enabled.

Procedure

1) Click **Administration** and select the organisation vDC.
2) Select **Org vDC Networks**, right click the organisation vDC network name and select **Configure Services**
3) Click the **VPN** tab and select **Add**
4) Type a name and optional description.
5) Select **a network in another organisation** from the drop-down menu.
6) Click **Connect to another organisation**, type the login information for the peer organisation, and click **Continue**.

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

7) Select a peer network.
8) Review the tunnel settings and click **Connect**.

The platform configures both peer network endpoints.

3.2.1.8 Create a VPN Tunnel to a Remote Network

An organisation administrator can create a VPN tunnel between an organisation network and a remote network. 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

Prerequisites

- A routed organisation vDC network (that connects externally)
- a routed remote network that uses IPSec.

Procedure

1) Click **Administration** and select the organisation vDC.
2) Select **Cloud Resources > Networks**
3) Click the **Organisation vDC Network** tab, right click the organisation vDC network name and select **Configure Services**
4) Click the **VPN** tab and select **Add**
5) Type a name and optional description.
6) Select **a remote network** from the drop-down menu.
7) Type the peer settings.
8) Review the tunnel settings and click **OK**.

The platform configures the organisation peer network endpoint.

What to do next

Manually configure the remote peer network endpoint. The remote peer will need to be compatible with the following settings:

Mode:	Main
Authentication Method:	Pre-Shared Key
Phase 1 Encryption:	AES-256
Phase 1 Authentication:	SHA1
Phase 1 DH Group:	2
Phase 1 Keylife:	28800
Phase 2 Encryption:	AES-256
Phase 2 Authentication:	SHA1
Phase 2 DH Group:	2
Phase 2 Keylife:	3600
Perfect Forward Secrecy:	On/Enabled

3.2.1.9 Enable Static Routing for an Organisation vDC Network

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

Prerequisites

- A routed organisation network (see 3.2 Managing Organisation vDC Networks)

Procedure

1) Click **Administration**.
2) Select **Cloud Resources > Networks**.
3) Right-click the organisation vDC network name and select **Configure Services**.
4) On the **Static Routing** tab, select **Enable static routing** and click **OK**.

What to do next

Create static routes.

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

An organisation administrator can add static routes between two vApp networks that are routed to the same organisation vDC network. Static routes allow traffic between the networks. You cannot add static routes between overlapping networks or fenced vApps. After you add a static route to an organisation vDC network, configure the network firewall rules to allow traffic on the static route. For vApps with static routes, you should 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

- A routed organisation network (see 3.2 Managing Organisation vDC Networks)
- Static routing is enabled on the organisation network (see 3.2.1.9 Enable Static Routing for an Organisation vDC Network)
- Two vApp networks routed to the organisation network (see 8.14 Working with Networks in a vApp)
- 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 organisation vDC network name and select **Configure Services**.
4) On the **Static Routing** tab, click **Add**.
5) Type a name, network address, and next hop IP address

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

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 organisation vDC network to allow traffic between the vApp networks. You can use information about the vApp networks to create the static routes.

Table 3-3. 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 3-4. Static Routing Settings

Network	Route Name	Network	Next Hop IP address	Route
vApp Network 1	Tovapp1	192.168.1.0/24	192.168.0.100	Within this network
vApp Network 2	Tovapp2	192.168.2.0/24	192.168.0.101	Within this network

What to do next

- Create firewall rules to allow traffic on the static routes (see 3.2.1.3 Add a Firewall Rule to an Organisation vDC Network)
- Review the other aspects of 3.2 Managing Organisation vDC Networks
- Review aspects of 8.14 Working with Networks in a vApp
- Review sample network configurations in Appendix A - sample vApp network configurations

3.2.1.11 Add Static Routes Between vApp Networks Routed to Different Organisation vDC Networks

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

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

Static routes 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

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

Procedure

1) Click **Administration** and select the organisation vDC
2) Click the **Org vDC Networks** tab, tight click the organisation vDC network name, and select **Configure Services**

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

   The network address is for the vApp network to which you want to add a static route. The next hop IP address is the external IP address of the router for the organisation vDC 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 organisation vDC 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 3 through Step 8 to add static routes to the second organisation vDC network.

Example: Static Routing Example
vApp Network 1 is routed to Org vDC Network 1. vApp Network 2 is routed to Org vDC Network 2. You can create static routes on the organisation vDC networks to allow traffic between the vApp networks. You can use information about the vApp networks and organisation vDC networks to create the static routes.

Table 3-5. 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 3-6. 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	192.168.0.101	Within this network

Table 3-7. Static Routing Settings for Org vDC Network 2

Network	Route Name	Network	Next Hop IP address	Route
vApp Network 1	Tovapp1	192.168.1.0/24	10.112.205.101	To external network
vApp Network 2	Tovapp2	192.168.11.0/24	192.168.10.100	Within this network

What to do next

- Create firewall rules to allow traffic on the static routes (see 3.2.1.3 Add a Firewall Rule to an Organisation vDC Network)
- Review the other aspects of 3.2 Managing Organisation vDC Networks
- Review aspects of 8.14 Working with Networks in a vApp
- Review sample network configurations in Appendix A - sample vApp network configurations

3.2.2 Reset an Organisation vDC Network

If the network services, such as DHCP settings, firewall settings, and so on, that are associated with an organisation network are not working as expected, reset the network. You are an organisation administrator. **CAUTION:** No network services are available while an organisation network resets, however if this operation is performed with the Organisation vDC network running normally, although the re-deployment is performed inline this operation will still result in a small outage.

Prerequisites

- An external NAT-routed organisation vDC network or an internal organisation vDC network.
- You are an organisation administrator.

Procedure

1) Click **Administration** and select the organisation vDC
2) Right click the organisation vDC network and select **Reset Network**
3) Click **Yes**.

3.2.3 View IP Usage for an Organisation vDC Network

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

Prerequisites

- You are an organisation administrator.

Procedure

1) Click **Administration** and select the organisation vDC
2) Right click the organisation vDC network and select **IP Allocations**

3.2.4 Add IP Addresses to an Organisation vDC Network IP Pool

If your externally organisation vDC network is running out of IP addresses, you will need to contact Manx Telecom for additional addresses to be provisioned.

3.2.5 View vApps and vApp Templates That Use an Organisation vDC Network

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

Prerequisites

- You are an organisation administrator.

Procedure

1) Click **Administration** and select the organisation vDC
2) Right click the organisation vDC network and select **Connected vApps**
3) Click **OK**

3.2.6 View Syslog Server Settings for an Organisation vDC or vApp Network

You can view the syslog server settings for a routed organisation vDC network.
You are an organisation administrator. All networks by default will be configured to log to a pair of syslog addresses as follows:

```
Syslog server 1 172.16.255.2
Syslog server 2 172.16.255.3
```

If an organisation vDC network or vApp network does not have any syslog server settings, then you can synchronize the network with the most current syslog server settings. See 3.2.7 Apply Syslog Server Settings to an Organisation vDC Network. If there is still a problem after you synchronize, contact us.

Prerequisites

- An external NAT-routed organisation vDC network.
- You are an organisation administrator

Procedure

1) Click **Administration** and select the organisation vDC
2) Click the **Org vDC Networks** tab, right click the organisation vDC network name, and select **Properties**
3) Click the **Syslog Server Settings** tab.

What to do next

Deploy the syslog vApp to add syslog hosts with the addressing above to your Cloud. See 3.2.8 Deploying syslog vApp template to enable syslog for firewalls.

3.2.7 Apply Syslog Server Settings to an Organisation vDC Network

You apply syslog server settings to a routed organisation vDC or vApp network to enable firewall rule logging. See 3.2.6 View Syslog Server Settings for an Organisation vDC or vApp Network for information on the addressing of the destination syslog hosts.

Prerequisites

- An external NAT-routed organisation vDC or vApp network

Procedure

1) Click **Administration** and select the organisation vDC
2) Click the **Org vDC Networks** tab, right click the organisation vDC network name, and select **Synchronize syslog server settings**
3) Click **Yes**

What to do next

Deploy the syslog vApp to add syslog hosts with the addressing above to your Cloud See 3.2.8 Deploying syslog vApp template to enable syslog for firewalls.

3.2.8 Deploying syslog vApp from template to enable syslog for firewalls

To enable the logging of firewalls from vShield edge devices inside Organisation vDC or vApp networks, it is possible to deploy a preconfigured vApp template that contains two syslog hosts. The addressing for these hosts is described in 3.2.7 Apply Syslog Server Settings to an Organisation vDC or vApp Network

Prerequisites

- An external NAT-routed organisation or vApp network

Procedure

The procedure is describe in detail over the next five sub sections

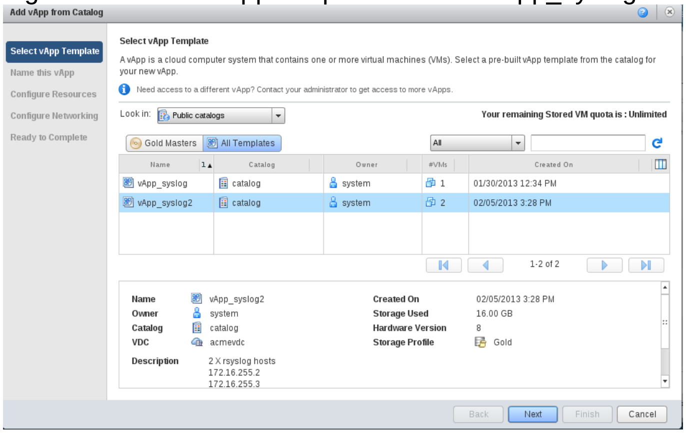
1) Add the syslog vApp
2) Connect the syslog vApp to the routed organisation network
3) Add a static route
4) Add a static route to any internal VSEs on vApp networks)
5) Configuring firewall logging as required

3.2.8.1 Add the syslog vApp

1) Navigate to the “My Cloud” tab and click on the ✚ symbol to “Add vApp from catalog”.

2) Choose “Public Catalogs” from the “Look in:” drop down and click “All Templates”

3) Right click on the vApp template named "vApp_syslog" and click Next



Add vApp from Catalog

Select vApp Template

A vApp is a cloud computer system that contains one or more virtual machines (VMs). Select a pre-built vApp template from the catalog for your new vApp.

Need access to a different vApp? Contact your administrator to get access to more vApps.

Look in: Public catalogs

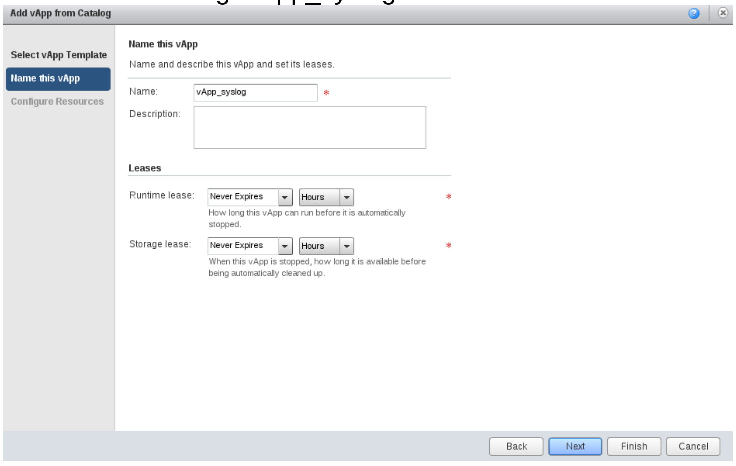
Your remaining Stored VM quota is : Unlimited

Name	Catalog	Owner	#VMs	Created On
vApp_syslog	catalog	system	1	01/30/2013 12:34 PM
vApp_syslog2	catalog	system	2	02/05/2013 3:28 PM

1-2 of 2

Name	vApp_syslog2	Created On	02/05/2013 3:28 PM
Owner	system	Storage Used	16.00 GB
Catalog	catalog	Hardware Version	8
VDC	acmevdc	Storage Profile	Gold
Description	2 X rsyslog hosts 172.16.255.2 172.16.255.3		

4) Provide a name e.g. vApp_syslog and click Next and Finish.



Add vApp from Catalog

Name this vApp

Name and describe this vApp and set its leases.

Name: vApp_syslog *

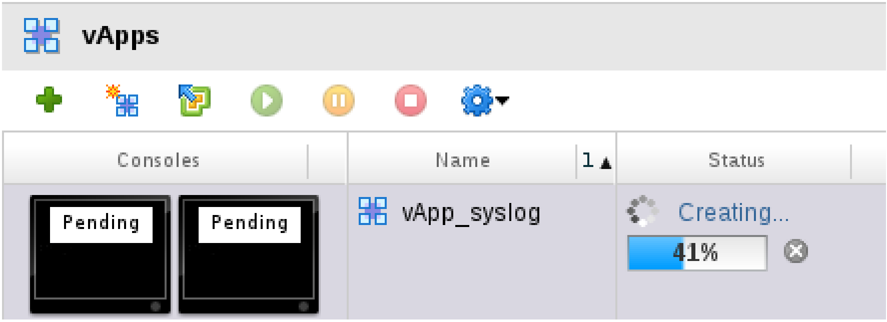
Description:

Leases

Runtime lease: Never Expires Hours *
How long this vApp can run before it is automatically stopped.

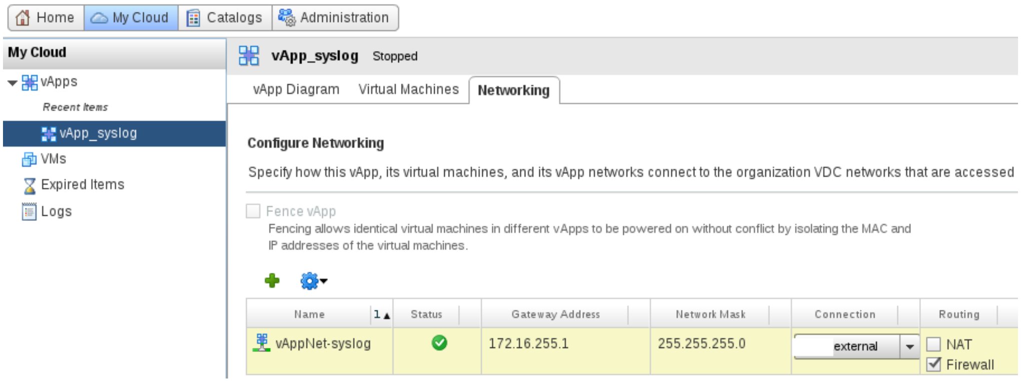
Storage lease: Never Expires Hours *
When this vApp is stopped, how long it is available before being automatically cleaned up.

5) Navigating to the "My Cloud" tab and selecting" vApps" on the left should now show the vApp being added. Wait until it has finished.



3.2.8.2 Connect the syslog vApp to the routed organisation network

1) Navigate to the "My Cloud" tab and select vApps on the left
2) click on the vApp that is named from step 4 and click on the “Networking” tab and check the box labelled “Show networking details”. A vApp network should be observed called “vAppNet-syslog”.
3) This will be currently disconnected, to connect it, select the Organisation vDC network for your vDC from the dropdown list under the “Connection” column. Click Apply, and once done, make sure **NAT** is **unchecked** and **Firewall** is checked and click Apply once more



Configure Networking

Specify how this vApp, its virtual machines, and its vApp networks connect to the organization VDC networks that are accessed

□ Fence vApp

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.

Name 1▲	Status	Gateway Address	Network Mask	Connection	Routing
vAppNet-syslog	✓	172.16.255.1	255.255.255.0	external	□ NAT ☑ Firewall

4) Right click on the vAppNet-syslog-network and select “Configure Services”
5) Click on the Firewall tab and enter in rules as follows (Note, these rules are recommended as they provide what is needed for logging, and also accessing the syslog servers via SSH from other vApps.

Name	src	src port	dst	dst port	proto	action	log
syslog syslog01	any	any	172.16.255.2	514	UDP	allow	no
syslog syslog02	any	any	172.16.255.3	514	UDP	allow	no
ssh syslog01	any	any	172.16.255.2	22	TCP	allow	yes
ssh syslog02	any	any	172.16.255.2	22	TCP	allow	yes

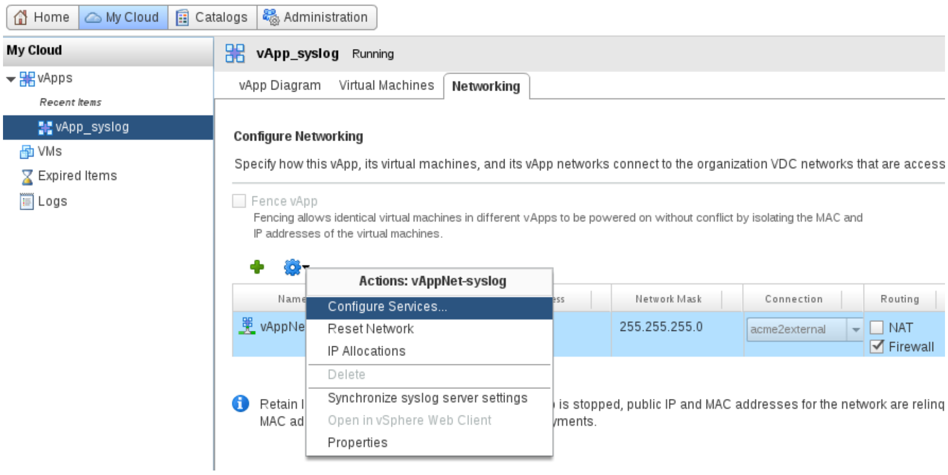
6) Click OK on the Configure Services dialog and click Apply to save the configuration.

7) The vApp will now require starting so that the vShield edge device can be assigned an IP address from the pool in the Organisation vDC network. Click on the “vApp

Diagram" tab and click the power on icon to start the vApp. This will take approx 5 minutes for the vShield Edge for the vAppp to be commissioned, started and configured. Once the vApp is started, go to the next step to configure static routes.

3.2.8.3 Configure static route to the syslog from the External network

1) Go back to the Networking tab and establish the IP address that has been assigned in the external network for the vShield edge device by right clicking the syslog internal network and selecting "Configure Services". More information on adding static routes can be found in 3.2.1.13 Enable Static Routing for an Organisation Network.



Configure Networking

Specify how this vApp, its virtual machines, and its vApp networks connect to the organization VDC networks that are access

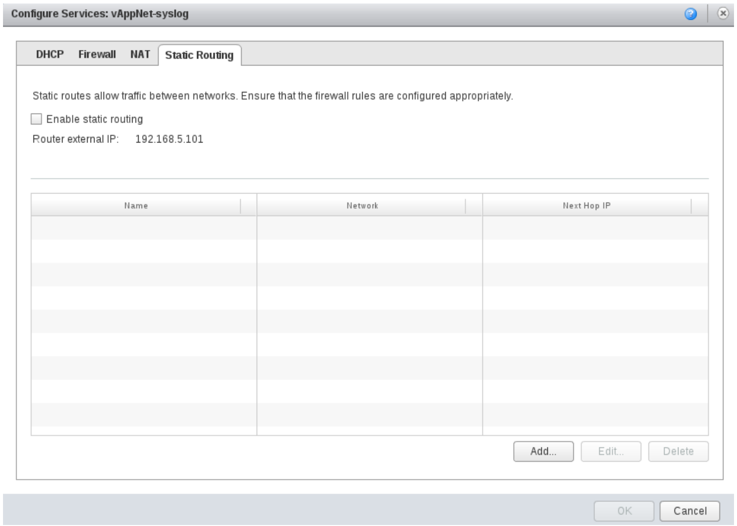
□ Fence vApp

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.

Name	ss	Network Mask	Connection	Routing
vAppNe		255.255.255.0	acme2external	□ NAT ☑ Firewall

Retain I … is stopped, public IP and MAC addresses for the network are relinq
MAC ad … yments.

2) Click on the "Static Routing" tab, and this will show the IP address (in this example it is 192.168.5.101). Click on Cancel once the IP is known.



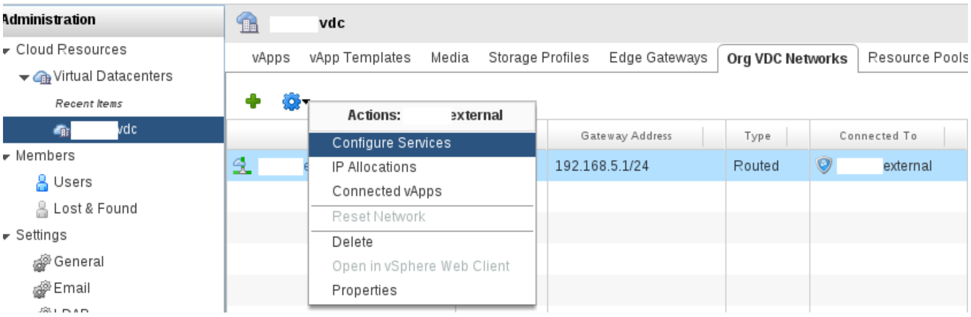
Static routes allow traffic between networks. Ensure that the firewall rules are configured appropriately.

□ Enable static routing

Router external IP: 192.168.5.101

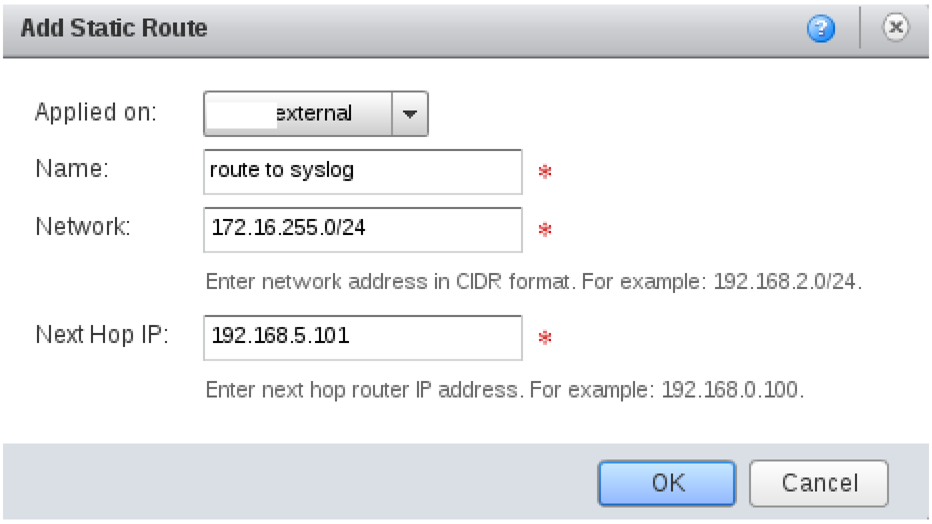
Name	Network	Next Hop IP

3) Click on the Administration tab for your organisation and select the Org vDC Networks tab. Right click on the Organisation vDC Network that is the external network connected to in section 3.2.8.2 step 5 and select "Configure Services"



Gateway Address	Type	Connected To
192.168.5.1/24	Routed	external

4) Click on the Static Routing tab and if not already checked, check the checkbox labelled “Enable static routing”. Once done add a static route called “syslog network” that routes 172.16.255.0/24 via the IP address established in the previous step.


Add Static Route

Applied on: external

Name: route to syslog *

Network: 172.16.255.0/24 *

Enter network address in CIDR format. For example: 192.168.2.0/24.

Next Hop IP: 192.168.5.101 *

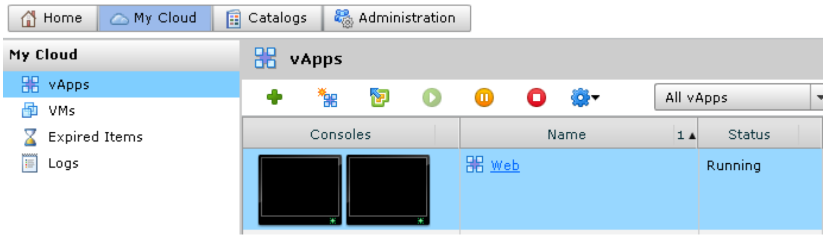
Enter next hop router IP address. For example: 192.168.0.100.

3.2.8.4 Adding Static routes for any other vApp networks

If any of your vApps have internal vApp networks, these can be configured to log to syslog as well. The only constraint is that they are connected to the same external network, and a static route is applied enabling the connectivity.

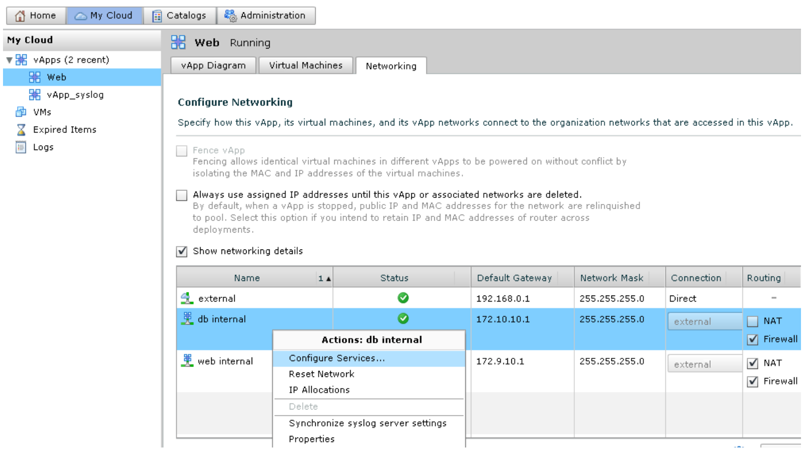
To apply a static route to an internal vApp network, complete as follows. (the example below is for a vApp network entitled “db internal”).

1) Navigate to the “My Cloud” tab and select vApps on the left. Locate the vApp where the internal network is located and click on its name



Consoles	Name	Status
	Web	Running

2) Click on the “Networking” tab, check the “Show networking details” checkbox and right click on the internal network that needs to be configured and select “Configure Services”.



Configure Networking

Specify how this vApp, its virtual machines, and its vApp networks connect to the organization networks that are accessed in this vApp.

□ Fence vApp
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.

□ Always use assigned IP addresses until this vApp or associated networks are deleted.
By default, when a vApp is stopped, public IP and MAC addresses for the network are relinquished to pool. Select this option if you intend to retain IP and MAC addresses of router across deployments.

☑ Show networking details

Name 1 ▲	Status	Default Gateway	Network Mask	Connection	Routing
external	✓	192.168.0.1	255.255.255.0	Direct	–
db internal	✓	172.10.10.1	255.255.255.0	external	□ NAT ☑ Firewall
web internal		172.9.10.1	255.255.255.0	external	☑ NAT ☑ Firewall

3) Under the Static routing tab, add in the static route in the same way as seen in section 5.3 step 3. Perform this section again on any other internal vApp networks that firewall logs are to be sent for.

3.2.8.5 Configure Firewall logging

So that the organisation or vApp network can actually log rules, the firewall must be configured to log and/or rules that are applied in the firewall need to be set to log. See section 3.2.1.3 Add a Firewall Rule to an Organisation Network for details on how to do this when adding a new rule.

3.2.8.6 Accessing the syslog machines with SSH

It is possible to access the machines using SSH, but note that as the vApp network for the syslog machines does not use NAT, the following conditions must be met:

a) The machine making the connection is within the External network
b) The machine making the connection has a static route inside the guest to route to 172.16.255.0/24 via the address identified in section 3.2.8.3 Configure static route to the syslog from the External network step 3.

3.2.9 Managing Expired Items

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

3.2.9.1 Manage Expired vApps

You can display a list of expired vApps, delete them, or restore them to your organisation. The organisation policy for what to do when a vApp storage lease expires is set to **Move to Expired Items**. See “Configure Organisation Lease, Quota, and Limit Settings,” on page 40.

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.

3.2.9.2 Manage Expired vApp Templates

You can display a list of expired vApp templates and delete them or restore them to your organisation. You are an organisation administrator. The organisation policy for what to do when a vApp template storage lease expires is set to **Move to Expired Items**. See "Configure Organisation Lease, Quota, and Limit Settings

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.

4 Working in an Organisation

Manx Telecom will create your organisation and assign the organisation administrator to it. We will then impart the URL of the organisation to the organisation administrator, who can login to the organisation and set it up. In the Home page the organisation administrator clicks the **Set up the Organisation** link to assign resources and manage a variety of operations on the organisation.

This chapter includes the following topics:

4.1 Understanding Leases

Creating an organisation involves specifying leases. Leases provide a level of control over an organisation'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, the platform 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, the platform marks the vApp or vApp template as expired, or deletes the vApp or vApp template, depending on the organisation policy that is configured.

For more information about specifying lease settings, see 4.2.4 Configure Organisation Lease, Quota, and Limit Settings. Users can configure email notification to receive a message before a runtime or storage lease expires. See 1.6 Set User Preferences, for information about lease expiration preferences.

4.2 Set Up an Organisation

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

Prerequisites

- You are an organisation administrator.

Procedure

1) 4.2.1 Change the Organisation Full Name
   You can change the full name of an organisation. This name appears in the Cloud Director application header when users log in.

2) 4.2.2 Add Users to the Organisation
   Every organisation should have at least one local organisation administrator account, so that users can log in.

3) 4.2.3 Configure Email Preferences
   The platform requires an SMTP server to send user notification and system alert emails. There is a default server provided, it is recommended to use this and leave this setting as-is.

4) 4.2.4 Configure Organisation Lease, Quota, and Limit Settings
   Leases, quotas, and limits constrain the ability of organisation users to consume storage and processing resources. Use these settings to prevent users from depleting or monopolizing an organisation's resources.

4.2.1 Change the Organisation Full Name

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

Prerequisites

- You are an organisation administrator.

Procedure

1) On **Name this Organisation** page, in the **Organisation full name**, type the new full name.
2) (Optional) Type a description of the organisation.
3) Click **Next.**

4.2.2 Add Users to the Organisation

Every organisation will have at least one local organisation administrator account. Additional users may be added.

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 VMs and click **OK**.

   These quotas limit the user's ability to consume storage and compute resources in the organisation.
6) Click **Next**.

4.2.3 Configure Email Preferences

The platform requires an SMTP server to send user notification and system alert emails. There is a default server provided, it is recommended to use this and leave this setting as-is.

Procedure

1) Select an SMTP server option.

Option	Description
Use system default SMTP server	The organisation uses the system SMTP server. (recommended)
Set organisation SMTP server	The organisation 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 organisation uses the system notification settings.
Set organisation notification settings	The organisation uses its own notification settings. Type an email address that appears as the sender for organisation emails, type text to use as the subject prefix for organisation emails, and select the recipients fororganisation 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**.

4.2.4 Configure Organisation Lease, Quota, and Limit Settings

Leases, quotas, and limits constrain the ability of organisation users to consume storage and processing resources. Use these settings to prevent users from depleting or monopolizing an organisation's resources. For more information about leases, see 4.1 Understanding Leases.

Procedure

1) Select the lease options for vApps and vApp templates.

   Leases provide a level of control over an organisation'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 organisation can store and power on in the organisation's virtual datacenters. The quotas that you specify act as the default for all new users added to the organisation.

3) Select the limits for resource intensive operations.

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

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

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

NOTE This setting does not affect Virtual Network Computing (VNC) or Remote Desktop Protocol (RDP) connections, those depend on the configuration of the guests.

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**.

4.3 Review Your Organisation Profile

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

Prerequisites

- You are an organisation administrator.

Procedure

1) Click **Administration**.
2) In the left pane, select **Settings > General**.
3) You can complete these operations.
    - Review your organisation's default URL.
    - Modify your organisation's full name.
    - Type a description.
4) Click **Apply**.

4.4 Modify Your Email Settings

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

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 organisation uses the system SMTP server. (recommended)
Set organisation SMTP server	The organisation 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 organisation uses the system notification settings.
Set organisation notification settings	The organisation uses its own notification settings. Type an email address that appears as the sender for organisation emails, type text to use as the subject prefix for organisation emails, and select the recipients for organisation 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**.

4.5 Modify Your Organisation's Policies

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

Prerequisites

- You are an organisation administrator.

Procedure

1) Select the lease options for vApps and vApp templates.

   Leases provide a level of control over an organisation'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 organisation can store and power on in the organisation's virtual datacenters. The quotas that you specify act as the default for all new users added to the organisation.

3) Select the limits for resource intensive operations.

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

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

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

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

5) (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**.

4.6 Set Default Domain for Organisation Virtual Machines

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

NOTE: for machines to be able to join domains, DHCP must be configured on the network that the domain member machines are to be connected to.

Prerequisites

- You are an organisation administrator.

Procedure

1) Click **Administration**.
2) In the left pane, select **Settings > Guest Personalization**.
3) Select the **Enable domain join for virtual machines in this organisation**.
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**.

4.7 Manage Users in Your Organisation

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

Prerequisites

- You are an organisation administrator.

Procedure

1) Click **Administration**.
2) In the left pane, select **Members > Users**.
   You can modify properties or roles.
3) Right-click the user and select **Properties**.
4) Make the necessary changes and click **OK**.

Your user settings are updated. See also 2 Managing Users

4.8 Manage Resources in Your Organisation

You must monitor and manage the resources you add to your organisation. You are an organisation administrator.

Procedure

1) Click **Administration**.
2) In the left pane, under **Cloud Resources**, select **Virtual Datacenters** or **Networks**.

The vDCs and networks in your organisation appear in the right pane. See also 3 Managing Cloud Resources.

4.9 Manage Virtual Machines in Your Organisation

You can manage virtual machines in your organisation. Virtual machines provide access to platform operations at the virtual machine console level.

Prerequisites

- You are an organisation administrator.

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 9 Working with Virtual Machines.

4.10 Viewing Organisation Log Tasks and Events

You can view tasks and events in your organisation to monitor and audit cloud activities. **Cloud Tasks** are long-running operations and their status changes as the task progresses. For example, a task's status generally starts as **Running**. When a task finishes, it's status changes to Successful or Error. **Cloud Events** are one-time occurrences that indicate an important part of an operation or a significant state change for a Cloud object. The platform also logs an event every time a user logs in, and notes whether the attempt was successful or not.

4.10.1 View Organisation Events

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

Prerequisites

- You are an organisation administrator.

Procedure

1) Click the **My Cloud**.
2) In the left pane, click **Logs**.
3) Click the **Events** tab.

   The platform displays information about each organisation-level event.

4) Double-click an event for more information.

4.10.2 View Organisation Tasks

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

Prerequisites

- You are an organisation administrator.

Procedure

1) Click **My Cloud**.
2) In the left pane, click **Logs**.
3) On the **Tasks** tab, you can examine the tasks in the organisation.
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, please contact us

5 Working with Catalogs (Catalogs)

A catalog is a container for vApp templates and media files in an organisation. Organisation administrators and catalog authors can create catalogs in an organisation. Catalog contents can then be shared with other users in the organisation. There are two types of catalogs; organisation catalogs and public catalogs.

Organisation catalogs include vApp templates and media files that you can share with other users in the organisation, but just that organisation. Public Catalogs are provided by Manx Telecom which are visible as read only to all organisation. Organisation administrators from any organisation on the platform can view the vApp templates and media files in these public catalog and either copy those files to a catalog in their own organisation for use by their members.

There are two ways to add vApp templates to a catalog. You can upload an OVF package directly to a catalog or save a configured vApp as a vApp template. For more information, see 7.4 Upload an OVF Package as a vApp Template and 7.10 Save a vApp as a vApp Template. You can also upload media files directly to a catalog. See 6.1 Upload Media Files.

Members of an organisation can access vApp templates and media files that they own or that are shared to them. Organisation administrators can share a catalog with everyone in an organisation, or with specific users and groups in an organisation. See 5.3 Share A Catalog.

This chapter includes the following topics:

5.1 Add a New Catalog

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

Prerequisites

- You are at least a catalog author.

Procedure

1) Click **Catalogs > My Organisation's Catalogs**.
2) On the **Catalogs** tab, click the **Add Catalog** button.
3) Type a catalog name and optional description and click **Next.**
4) (Optional) To share the catalog with members of the organisation, click **Add Members**, select users, select an access level, click **OK**, and click **Next**.
5) Review the summary Click **Finish**

5.2 Access a Catalog

You can access Manx Telecom provided catalogs (public catalogs).

- To access a public catalog, you must be an organisation administrator .
- To access a catalog in your organisation, you must be at least a vApp author.

Procedure

1) Click **Catalogs**.
2) In the left pane, click on a catalog option.
   - **My Organisation's Catalogs**
   - **Public Catalogs**
3) In the right pane, select a catalog, right-click, and select **Open**.

5.3 Share A Catalog

Share a catalog to make its contents available to users in your organisation. Users with the proper rights and access level can use vApp templates and media from the shared catalog to create their own vApps.

Prerequisites

- You are at least a catalog author.

Procedure

1) Click **Catalogs > My Organisation's Catalogs**.
2) Select a catalog, right-click, and select **Share**.
3) Click **Add Members**.
4) Select the users and groups with whom you want to share the catalog.

Option	**Action**
Everyone in the organisation	Select this option to share the catalog with everyone.
Specific users and groups	Select this option, click specific users and groups, and click **Add**.

5) Select an access level and click **OK**.

Option	**Action**
Read Only	Open, Add to My Cloud, Download, Copy to Catalog
Read/Write	Open, Add to My Cloud, Download, Copy to Catalog, Publish, Move to Catalog, Delete
Full control	Open, Add to My Cloud, Download, Copy to Catalog, Publish, Move to Catalog, Delete, Share

   The actual actions a user can perform on a catalog and its contents depends on the intersection of the rights of the user and their access level to the catalog. Sharing a catalog with full control does not grant a user rights that the user does not already have.

6) Click **OK**.

5.4 Change the Owner of a Catalog

You 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

- You are an organisation administrator.

Procedure

1) Click **Catalogs > My Organisation's Catalogs**.
2) On 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 their user name.
4) Click **OK**.

5.5 Delete a Catalog

You can delete a catalog from your organisation. You are at least a catalog author.

Prerequisites

- 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 **Catalogs**.
2) In the left pane, click **My Organisation's Catalogs**.
3) Select a catalog, right-click, and select **Delete**.
4) Click **Yes**.

The empty catalog is deleted from your organisation.

5.6 Modify the Properties of Your Catalog

You can review and modify your catalog properties.

Prerequisites

- You are at least a catalog author.

Procedure

1) Click **Catalogs**.
2) In the left pane, click **My Organisation's Catalogs**.
3) Select a catalog, right-click, and select **Properties**.
4) Review the properties in the **General**, **Sharing**, and **Publishing** tabs.
5) Modify the relevant properties and click **OK**.

Your catalog properties are updated.

5.7 Understanding Catalogs and Their Contents

A catalog consists of a list of catalogs, vApp templates, and media files in your organisation. When you click the **Catalogs** button in the menu bar, these tabs appear.

- **Catalogs**
- **vApp Templates**
- **Media**

If you are an organisation administrator, you can access published catalogs in the left pane.

5.7.1 Using vApp Templates in a Catalog

You can access vApp templates in a catalog in your organisation or, if you are an organisation administrator, from a published catalog. To access a vApp template in a catalog in your organisation, in the left pane, click **My Organisation's Catalogs** and click on the **vApp Templates** tab. Select a vApp template and right-click to see the operations you can complete.

5.7.2 Using Media Files in a Catalog

You can access media files in a catalog in your organisation (or, if you are a organisation administrator, a published catalog). To access a media file in a catalog in your organisation, in the left pane, click **My Organisation's Catalogs** and click on the **Media** tab. Select a media file and right-click to see the operations you can complete.

5.8 Working in Published Catalogs

Organisation administrators can access a published catalog and copy its vApp templates and media files to a catalog in their organisation. They can then share the organisation catalog with other members of their organisation so they can use the vApp templates and media files.

5.8.1 Accessing vApp Templates from a Public Catalog

You can access vApp templates from published catalogs and copy them to your catalog.

Prerequisites

- You are an organisation administrator.

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 an operation.
    - **Open**
    - **Add to My Cloud**
    - **Download**
    - **Copy to Catalog**
    - **Properties**

    You cannot modify properties until you copy the vApp template to your catalog. If you select A**dd to My Cloud**, the vApp template is saved and added as a vApp.

4) Click **OK**

.

The vApp template you selected is added to the specified catalog your organisation.

5.8.2 Accessing a Media File from a Public Catalog

You can access a media file from a published catalog and add it to your organisation.

Prerequisites

- You are an organisation administrator.

Procedure

1) Click **Catalogs**.
2) In the left pane, click **Public Catalogs**.
   Media files are available for use if they reside in the same vDC as your Cloud vApp.
3) On the **Media** tab, select a media file, right-click and select **Copy to Catalog**.
4) Click **OK**.

The media file is copied to your catalog.

What to do next

You can select the media file and complete a variety of operations on it, such as move it to another catalog in your organisation, delete it, or modify its properties.

6 Working with Media Files

A catalog will allow you to upload, copy, move, and edit the properties of media files.

This chapter includes the following topics:

6.1 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

- The computer from which you are uploading must have Java Plug-in 1.6.0_10 or later installed.
- You are at least a catalog author

Procedure

1) Click **Catalogs > My Organisation's Catalogs**.
2) On the **Media** tab, click the **Upload** button.
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.
5) This is the name that appears in the platform.
6) Select the destination vDC and catalog.
7) Click **Upload**.

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

6.2 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 log out of the platform and log in, transfer history is lost. You cannot resume the upload.
- The default timeout for pending transfer sessions is one hour. You can configure this value.
- 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

- You have initiated the upload or download of a media file.
- You are at least a catalog author.

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.

6.3 Copy Media Files to a Catalog

You can copy media files to another catalog. You are at least a catalog author.

Prerequisites

- You have access to multiple vDCs (by default an organisation will only be configured with one vDC).

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 and vDC.
5) Click **OK**.

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

6.4 Move Media Files to Another Catalog

You can move media files to another catalog in your organisation.
You are at least a catalog author.

Prerequisites

- You have access to multiple catalogs and vDCs (by default an organisation will only be configured with one vDC).

Procedure

1) Click **Catalogs**.
2) On the **Media** tab, select a media file, right-click, and select **Move To Catalog**.
3) Select a catalog and a vDC.
   The catalog you select must be in your organisation.
4) Click **OK**.

The media file is moved to the selected catalog

6.5 Delete Media Files

You can delete media files from your catalog.

Prerequisites

- You are at least a catalog author.

Procedure

1) Click **Catalogs > My Organisation's Catalogs**.
2) On the **Media** tab, select a media file, right-click, select **Delete**.
3) Click **Yes**.

The media file is deleted.

6.6 Modify Media File Properties

You can review and modify some properties of a media file. You are at least a catalog author.

Procedure

1) Click **Catalogs > My Organisation'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**.

7 Working with vApp Templates

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 organisation.

This chapter includes the following topics:

7.1 Open a vApp Template

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

Prerequisites

- You are at least a vApp user.

Procedure

1) Click **Catalogs**.
2) In the left pane, click on a catalog option.
   - **My Organisation's Catalogs**
   - **Public Catalogs**

   You can open vApp templates in your organisation's catalogs or, if you are an organisation administrator, from a MT provided public catalog.

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

7.2 Add a vApp Template to My Cloud

You can add a vApp template as a vApp from your catalog to **My Cloud**. You are at least a vApp author. 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

- A vApp template is available in a published or a locally shared catalog.

Procedure

1) Click **Catalogs**.
2) In the left pane, click on a catalog option.
   - **My Organisation's Catalogs**
   - **Public Catalogs**

You can access vApp templates in your organisation's shared catalogs or, if you are an organisation 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 runtime and storage lease and click **Next**.
6) Select a virtual datacenter, configure the virtual machines in the vApp, and click **Next**.
7) Configure the custom properties, if any, and click **Next**.
8) Configure the networking options for the vApp and click **Next**.
9) Review the vApp summary information and click **Finish**.

The platform will now create a vApp on the **My Cloud > vApps** page.

7.3 Download a vApp Template

You can download a vApp template from a catalog locally as an OVF file. You are at least a catalog author.

Prerequisites

- The computer from which you are downloading must have Java Plug-in 1.6.0_10 or later installed.

Procedure

1) Click **Catalogs**.
2) In the left pane, click on a catalog option.
   - **My Organisation's Catalogs**
   - **Public Catalogs**

   You can download vApp templates from your organisation's catalogs or, if you are an organisation 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 and click **Save**.
   You can click the **Launch Uploads and Downloads Progress Window** button from **My Organisation's Catalogs** to track the progress.

7.4 Upload an OVF Package as a vApp Template

You can upload an OVF package from remote shares and your local directory to the platform as a vApp template. You are at least a catalog creator. The platform will support OVFs uploads based on 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

- The computer from which you are uploading must have Java Plug-in 1.6.0_10 or later installed.
- For information about creating OVFs, see the *OVF Tool User Guide* and *VMware vCenter Converter 4.0.1User's Guide* at www.vmware.com
- The platform does not support uploading compressed OVF files.

Procedure

1) Click **Catalogs > My Organisation'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 vDC 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 9.22.2 Installing VMware Tools in a vApp.

7.5 Resume the Upload of a vApp Template

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

- You are at least a catalog creator.
- If you log out of the platform and log in, transfer history is lost. You cannot resume the upload.
- The default timeout for pending transfer sessions is one hour. You can configure this value up to one hour.
- 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

- You have initiated the upload or download of a vApp template.

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**.

7.6 Copy a vApp Template from a Public Catalog to an Organisation Catalog

You can copy a vApp template from a public catalog to your organisation catalog to make it available to users in your organisation. You are a vApp author or organisation administrator.

Prerequisites

- You have a catalog and vDC.

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 vDC.
   Select a shared catalog to give organisation users access to the template.
6) Click **OK**.

The platform copies the vApp template to the organisation catalog. The vApp appears on the **vApp Templates** tab in **My Organisation's Catalogs**.

7.7 Copy a vApp Template Between an Organisation's Catalogs

You can copy a vApp template from one catalog in your organisation to another catalog in the same organisation. 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. You are an organisation administrator, catalog author, or vApp author.

Prerequisites

- You must have access to at least two catalogs and a vDC with available space.

Procedure

1) Click **Catalogs > My Organisation'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 vDC.
5) Click **OK**.

7.8 Move a vApp Template Between an Organisation's Catalogs

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

Prerequisites

- You must have access to at least two catalogs and a vDC with available space.

Procedure

1) Click **Catalogs > My Organisation's Catalogs**.
2) On the **vApp Templates** tab, right-click a vApp template and select **Move To Catalog**.
3) Select a destination catalog and vDC.
4) Click **OK**.

The platform copies the source vApp template to the destination catalog and then deletes the source vApp template.

7.9 Delete a vApp Template

You can delete a vApp template from an organisation catalog. If the catalog is published, the vApp template
is also deleted from **Public Catalogs**.
You are at least a vApp author.

Procedure

1) Click **Catalogs > My Organisation'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.

7.10 Save a vApp as a vApp Template

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

Prerequisites

- You are at least a vApp author.
- Your organisation has a catalog and a vDC with available space.
- The vApp must be stopped.

Procedure

1) Click **My Cloud**.
2) In the left pane, click **vApps**.
3) Right-click a vApp and select **Add to Catalog**.
4) Type a name and optional description for the vApp template.
5) Select a vDC, a catalog, and a storage lease.
6) 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 must follow the guest operating system settings of the vApp template. If you select this option, and guest customization is enabled, the guest operating system is personalized.
Customize VM settings	Guest operating system is personalized regardless of the vApp template settings, and the guest operating system is personalized when the vApp is deployed. This option requires that a supported version of VMware Tools be installed on all virtual machines in the vApp.

7) Click **OK**.

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

7.11 Modify vApp Template Properties

You can modify some basic properties of a vApp template. To make more advanced changes to a vApp template, add it to **My Cloud**, make the changes, then add it back to the catalog as a new vApp template.

Prerequisites

- You are an organisation administrator.

Procedure

1) Click **Catalogs > My Organisation'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.
5)

   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 must follow the guest operating system settings of the vApp template. If you select this option, and guest customization is enabled, the guest operating system is personalized.
Customize VM settings	Guest operating system is personalized regardless of the vApp template settings, and the guest operating system is personalized when the vApp is deployed. This option requires that a supported version of VMware Tools be installed on all virtual machines in the vApp.

6) 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.

7) To reset the vApp template storage lease, select the **Reset lease** check box and select a new storage lease.
8) Click **OK**.

8 Working with vApps

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:

8.1 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 organisation administrators and vApp authors can access vApp templates in public catalogs.
- vApp users and above can access vApp templates in organisation 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 organisation'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) Configure the custom properties, if any, and click **Next**.
9) Configure the networking options for the vApp and click **Next**.
10) Review the vApp summary information and click **Finish**.

The platform creates a vApp in **My Cloud**.

8.2 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) 8.2.1 Complete the vApp Profile

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

2) 8.2.2 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.

3) 8.2.3 Configure the Virtual Machines

   Select the virtual datacenter (vDC) 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) 8.2.4 Configure Networks

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

8.2.1 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**.

8.2.2 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 organisation administrator or vApp author to access public catalogs.

Procedure

1) To add virtual machines from vApp templates, select **My organisation'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**.

8.2.3 Configure the Virtual Machines

Select the virtual datacenter (vDC) 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 vDC.
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**.

8.2.4 Configure Networks

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

8.3 Copy a vApp

To create a new vApp based on an existing vApp, you can copy a vApp and modify the copy to meet your needs. 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 **Copy to**.
4) Type a name and optional description.
5) Select a vDC.
6) Click **OK**.

What to do next

Modify the contents and properties of the new vApp.

8.4 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**.

8.5 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**.

8.6 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**.

8.7 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 labelled as **Stopped**.

8.8 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**.

8.9 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. Caution, a reset is akin to pulling the power from a machine, any guest will be forcibly stopped.

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**.

8.10 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.

8.11 Add Virtual Machines to a vApp

You can add virtual machines to a vApp. You must be an organisation administrator or vApp author to access virtual machines in public catalogs. 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 the VMware KB article at the following location: http://kb.vmware.com/kb/1001805.

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 organisation'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**.

8.12 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**.

8.13 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. You cannot enter negative numbers.
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 to wait between when you start a vApp and when The platform powers on each 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 to wait between when you stop a vApp and when The platform powers off or shuts down each virtual machine. 5 Click **OK**.

Example: Starting and Stopping Virtual Machines

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

Table 8-1 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.

8.14 Working with Networks in a vApp

The virtual machines in a vApp can connect to vApp networks (isolated or routed) and organisation 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 organisation vDC 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 organisation 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 organisation vDC network. If you have multiple vApps that contain identical virtual machines connected to the same organisation vDC 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.

See also:

- 3.2 Managing Organisation Networks
- 8.14 Working with Networks in a vApp
- Appendix A - sample vApp network configurations

8.14.1 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.

8.14.2 Adding Networks to a vApp

You can add vApp networks and Organisation vDC networks to a vApp

- 8.14.2.1 Add a vApp Network to a vApp
  Add a vApp network to a vApp to maike the network available to virtual machines in the vApp.

- 8.14.2.2 Add an organisation vDC Network to a vApp
  Add an organisation vDC network to a vApp to make the network available to virtual machines in the vApp.

8.14.2.1 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**.

   The platform creates an isolated vApp network and displays it in the network list.

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

   This routes the vApp network to the organisation network.

10) Click **Apply**.

What to do next
Connect a virtual machine in the vApp to the network.

8.14.2.2 Add an Organisation Network to a vApp

Add an organisation vDC 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 **Organisation vDC Network** and click **Next**.
6) Select an organisation network and click **Finish**.
   The platform adds the organisation network and displays it in the network list.
7) (Optional) Select the **Fence vApp** check box.

This changes the connection from **Direct** to **Fenced** for all organisation networks in the vApp. 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 organisation vDC's network pool. A vShield Edge is created and attached to both the isolated network and the organisation vDC network. Traffic going to and from the virtual machines pass through vShield Edge, 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

8) Click **Apply**.

What to do next
Connect a virtual machine in the vApp to the network.

8.14.3 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 8-1. Network Services Available by Network Type

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

8.14.3.1 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, the platform 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.

   The platform 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 max lease time or use the default values and click **OK**.
8) Click **Apply** which update 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

8.14.3.2 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 8.14.3.3 Add a Firewall Rule to a vApp Network.

You can log events related to the default firewall action. For information about applying syslog server settings, see 8.14.11 Apply Syslog Server Settings to a vApp Network. To view the current syslog server settings see 8.14.10 View Syslog Server Settings for a vApp Network.

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**.
6) Select the default firewall action.
   Allow – Allow all traffic except when overridden by a deny firewall rule
   Deny – Block all traffic except when overridden by an allow firewall rule
7) (Optional) Select the **Log** check box to log events related to the default firewall action.
8) Click **OK**.
9) Click **Apply**.

8.14.3.3 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. In order for a firewall rule to be enforced, you must enable the firewall for the vApp network. See 8.14.4.2 Enable the Firewall for a vApp Network. When you add a new firewall rule to a vApp network, it appears at the bottom of the firewall rule list. See 8.14.4.4 Reorder Firewall Rules for a vApp Network for information about setting the order in which firewall rules are enforced.

It is possible to log firewall rule events. For information about applying syslog server settings, see 8.14.11 Apply Syslog Server Settings to a vApp Network. To view the current syslog server settings see 8.14.10 View Syslog Server Settings for a vApp Network.

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) (Optional) select Match rule on translated IP to have the rule check against translated IP addresses rather than original IP addresses and choose traffic direction to apply this rule on
8) Type the traffic **Source**

Option	Description
IP address	Type a source IP address to apply the rule on (e.g 192.168.0.100)
Range of IP addresses	Type a range of source IP addresses to apply this rule on (e.g. 192.168.0.100 – 192.168.0.150)
CIDR	Type the CIDR notation of traffic to apply this rule on (e.g. 192.168.0.0/24)
Internal	Apply this rule to internal traffic only
External	Apply this rule to external traffic only
Any	Apply this rule to traffic from any source

For incoming traffic, the source is the external network. For outgoing traffic, the source is the organisation vDC network.

9) Select a **Source port** from the drop-down menu

10) Type the traffic **Destination**

Option	Description
IP address	Type a source IP address to apply the rule on (e.g 192.168.0.100)
Range of IP addresses	Type a range of source IP addresses to apply this rule on (e.g. 192.168.0.100 – 192.168.0.150)
CIDR	Type the CIDR notation of traffic to apply this rule on (e.g. 192.168.0.0/24)
Internal	Apply this rule to internal traffic only
External	Apply this rule to external traffic only
Any	Apply this rule to traffic from any source

11) Select the **Destination port** to apply this rule on from the drop-down menu
12) Select the **Protocol** to apply this rule on from the drop-down menu
13) Select the action (A firewall rule can allow or deny traffic that matches a rule)
14) Select the **Enabled** check box
15) (Optional) Select the **Log network traffic for firewall rule** check box.

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

16) Click **OK** and **OK** again.
17) Click **Apply**

8.14.3.4 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**.

8.14.3.5 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 organisation network. When you enable IP masquerade, the platform translates a virtual machine's private, internal IP address into a public IP address for outbound traffic.

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 and select **Port Forwarding**.
6) Select **Enable IP Masquerade** and click **OK**.
7) Click **Apply**.

8.14.3.6 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, the platform 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 8.14.3.8 Reorder Port Forwarding Rules for a vApp Network.

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**.

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

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 **IP Translation**, and click **Add**.
6) Select a VM interface and mapping mode and click **OK**.
   For **Manual** mapping mode, type an external IP address.
7) Click **OK** and click **Apply**.

8.14.3.8 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**.

8.14.3.9 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.

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.

8.14.3.10 Add Static Routes to vApp Networks

You can add static routes between two vApp networks that are routed to the same organisation 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, you should select the **Always use assigned IP addresses until this vApp or associated networks are deleted** check box.

Static routes only function 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

- Two vApp networks routed to the same organisation 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) On the **Networking** tab, select **Show networking details**.
4) Right-click the vApp network and select **Configure Services**.
5) On the **Static Routing** tab, 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 you want to add a static route. The next hop IP is the external IP address of that vApp network's router.
7) Click **OK** and click **Apply**.
8) 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.

Table 8-2. 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 8-3. 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.

8.14.4 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 organisation administrator can reset the network. Network services are not available for VMs connected to this vApp network during the reset. The process takes approx 3-5 minutes.

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**.

8.14.5 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**.

8.14.6 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**.

8.14.7 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**.

8.14.8 Configure IP Address Persistence

By default, when you stop a running vApp or power off a virtual machine, the platform releases any IP and MAC addresses the virtual machines were using. You can configure a vApp to retain the network addresses of its virtual machines until the vApp, VM, or network is deleted. Static routing relies on the IP addresses of the virtual machines and virtual routers 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) Select a vApp, right-click, and select **Open**.
4) On the **Networking** tab, select the **Always use assigned IP addresses...**check box and click **Apply**.

The virtual machines in the vApp keep their assigned IP and MAC addresses, even when they are powered off.

8.14.9 View Syslog Server Settings for a vApp Network

You can view the syslog server settings for a routed vApp network. You are an organisation administrator. All networks by default will be configured to log to a pair of syslog addresses as follows:

```
Syslog server 1 172.16.255.2
Syslog server 2 172.16.255.3
```

If a vApp network does not have any syslog server settings, then you can synchronize the network with the most current syslog server settings. See 8.14.11 Apply Syslog Server Settings to a vApp Network. If there is still a problem after you synchronize, contact us.

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.

What to do next

Deploy the syslog vApp to add syslog hosts with the addressing above to your Cloud See 3.2.8 Deploying syslog vApp template to enable syslog for firewalls.

8.14.10 Apply Syslog Server Settings to a vApp Network

You can apply syslog server settings to a vApp network to enable firewall rule logging. See 8.14.9 View Syslog Server Settings for a vApp Network for information on the addressing of the destination syslog hosts.

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**.

8.15 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.

- 8.15.1 Modify a vApp Name and Description
  You can change the name and description associated with a vApp to make is more meaningful

- 8.15.2 Modify vApp OVF Environment Properties
  If a vApp includes user-configurable OVF environment properties, you can review and modify those properties

- 8.15.3 Reset vApp Leases
  You can reset the runtime and storage leases for a vApp

- 8.15.4 Share a vApp
  You can share your vApps with other groups or users in your organisation. The access controls you set dfetermine the operations that can be completed on the shared vApps.

8.15.1 Modify a vApp Name and Description

You can change the name and description associated with a vApp to make it more meaningful.

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 **General** tab, modify the vApp name and description and click **OK**.

8.15.2 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**.

8.15.3 Reset vApp Leases

You can reset the runtime and storage leases for a vApp.

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 **General** tab, select the **Reset leases** check box, select a runtime and storage lease, and click **OK**.

8.15.4 Share a vApp

You can share your vApps with other groups or users in your organisation. 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 organisation	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	**Action**
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.

8.16 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** pages, 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.

8.17 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.

Prerequisites

- You are an organisation 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.

8.18 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. The platform supports hardware version 7, and hardware version 8 virtual machines. 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**.

8.19 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 vDC and catalog.
6) In the **Storage lease:** drop-down menu, select when you would like the vApp template to expire.
7) Select an option.

Option	Action
Make Identical Copy	vApps that are created from this vApp template must follow the guest operating system settings of the vApp template. If you select this option, and guest customization is enabled, the guest operating system is personalized.
Customize VM Settings	Guest operating system is personalized regardless of the vApp template settings, and the guest operating system is personalized when the vApp is deployed.

8) Click **OK**.

The vApp is saved as a vApp template in the selected catalog.

8.20 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**

8.21 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 **OK**

8.22 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 **OK**

8.23 Copy a vApp to Another vDC

When you copy a vApp to another vDC, the original vApp remains in the source vDC

Prerequisites

Your organisation has been configured with two or more vDCs
You are at least vApp author for the destination vDC

Procedure

1) Select **My Cloud**
2) In the left pan, click vApps,
3) Select a vApp, right-click and select **Copy to.**
4) Type a name and description
5) Select a destination vDC
6) Click **OK**

The new vDC for this vApp appears in the **vDC** column on the **vApps** page.

8.24 Move a vApp to Another vDC

When you movea vApp to another vDC, the original vApp is removed from the source vDC

Prerequisites

Your organisation has been configured with two or more vDCs
You are at least vApp author for the destination vDC
The vApp in the source vDC is stopped

Procedure

1) Select **My Cloud**
2) In the left pan, click vApps,
3) Select a vApp, right-click and select **Move to**.
4) Select a destination vDC
5) Click **OK**

8.25 Delete a vApp

You can delete a vApp, which removes it from your organisation.
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**.

9 Working with Virtual Machines

Virtual machines have a guest operating system on which you can install and run any software supported by that operating system. Within your cloud, you can install VMware Tools, insert DVDs and floppy disks, and remotely connect to virtual machines.

These are the most basic operations that you can do on a virtual machine.

- **Power On**, which is equal to powering on a physical machine.
- **Power Off**, which is equal to powering off a physical machine.
- **Suspend**, where the CPU of a deployed virtual machine is frozen. You can suspend a machine when you need to leave a virtual machine but do not want to lose its current state.
- **Reset**, which power cycles the virtual machine.

This chapter includes the following topics:

9.1 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 may be required to install VMware Remote Console Plug-In. Click **Install** 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.

9.2 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**.

9.3 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**.

9.4 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**.

9.5 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**.

9.6 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**.

9.7 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**.

9.8 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 .iso 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.

9.9 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.

9.10 Insert a Floppy

You can access floppy disk images from catalogs to use in a guest operating system. When you insert a floppy disk, you can install operating systems, applications, drivers, and so on.

Prerequisites

- You have .flp media files 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 Floppy from Catalog**.
4) Using the drop-down menu, select a floppy disk image or select one from the list and click **Insert**.

The selected floppy disk is inserted.

9.11 Eject a Floppy

After you have finished using a floppy disk 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 Floppy**.

The floppy disk is removed from the virtual machine.

9.12 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 platform supports hardware version 7, and hardware version 8 virtual machines. You cannot downgrade the hardware version of a virtual machine.

Prerequisites

- The virtual machine must be powered off and it must have 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**.

9.13 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 R**emote 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**.

9.14 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) Click **My Cloud** > **VMs**
2) Right click the **VM** and select **Create Snapshot**
3) Click **OK**.

Note: changes to the VM's disk(s) will be stored in sparse Copy-On-Write files, all of which will count to the storage resource usage as they grow (when changes are made to the disk(s) of the VM). If the "snapshot the memory of the virtual machine" is chosen, the current running memory is also stored as a file.

9.15 Revert a Virtual Machine to a Snapshot

You can revert a virtual machine to the state is was in when the snapshot was created

Prerequisites

- Verify that the virtual machine has a snapshot

Procedure

1) Click **My Cloud** > **VMs**
2) Right click the **VM** and select **Revert to Snapshot**
3) Click **Yes**.

The sparse files written to since the snapshot was taken will be zeroed. If the "snapshot the memory of the virtual machine" option was chosen for the snapshot being reverted, the machine's state will return to that point, otherwise the machine will be placed in a powered off state.

9.16 Remove a Snapshot of a Virtual Machine

You can remove a snapshot of a virtual machine which will permanently remove that snapshot and merge all changes made since into the disk(s) of the VM.

Prerequisites

- Verify that the virtual machine has a snapshot

Procedure

4) Click **My Cloud** > **VMs**
5) Right click the **VM** and select **RemoveSnapshot**
6) Click **Yes**.

The sparse files that contained any changes to the VM's disk will be merged into the base disks and any memory bitmap recorded for this snapshot will be removed.

9.17 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

7) Click **My Cloud**.
8) In the left pane, click **VMs**.
9) Select a virtual machine, right-click, and select **Copy to** or **Move to**.
10) Follow the prompts to complete the wizard.
11) Click **Finish**.

9.18 Delete a Virtual Machine

You can delete a virtual machine from your organisation. Note vApps can exist with no virtual machines left in them.

Prerequisites

- The virtual machine in question must be powered off.

Procedure

1) Click **My Cloud**.
2) In the left pane, click **VMs**.
3) Select the appropriate **VM**, right-click, and select **Delete**.
4) Click **Yes**.

9.19 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.

- 9.19.1 Modify Virtual Machine General Properties
  You can review and modify the name, description and other general properties of a virtual machine

- 9.19.2 Modify Virtual Machine CPUs and Memory
  You can modify the number of virtual CPUs and memory for a virtual machine.

- 9.19.3 Modify Virtual Machine OVF Environment Properties
  If a virtual machine includes user-configurable OVF environment properties, you can review and modify those properties

- 9.19.4 Configuring Virtual Machine Resource Allocation Settings
  Reservation pool vDCs support the ability to control resources allocation at the virtual machine level. Users with the necessary rights can customise the amount of resources that are allocated to their virtual machines.

- 9.19.5 Modifying Virtual Machine Hard Disks
  You can add hard disks, edit hard disks , and delete hard disks from a virtual machine

- 9.19.6 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.

9.19.1 Modify Virtual Machine General Properties

You can review and modify the name, description, and other general properties of a virtual machine.

Prerequisites

- The virtual machine must be powered off to modify some general properties.

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 **General** tab, modify the properties and click **OK**.

Option	Description
Full name	The display name of the virtual machine in the vDC.
Computer name	The computer/host name set in the guest operating system that identifies the VMon a network. Note: this field is restricted to 15 chars because of a Windows OS limitation.
Description	An optional description of the virtual machines.
Operating System Family	Drop-down list containing supported operating system families.
Operating System	Drop-down list containing supported operating systems.
Virtual hardware version	The virtual hardware version of the VM.
Virtual CPU hot add	Select the check box to enable virtual CPU hot add. This allows you to add virtual CPUs to a powered on VM. (only supported on certain guest OS and VM hardware versions.
Memory hot add	Select the check box to enable memory hot add. This allows you to add memory to a powered on VM. (only supported on certain guest OS and VM hardware versions.
Synchronize time	Select the check box to enable time synch between the VM OS and the vDC.

9.19.2 Modify Virtual Machine CPUs and Memory

You can modify the number of virtual CPUs and memory for a virtual machine. The number of virtual CPUs and memory that a virtual machine supports depends on its virtual hardware version.

Table 9-1. Virtual Hardware Versions and CPU/Memory Support

Virtual Hardware Version	Maximum CPUs	Maximum Memory
HW4	4	64GB
HW7	8	255GB
HW8	32	1011GB

You must power off the virtual machine before adding CPUs or memory, unless the virtual machine supports memory hot add and virtual CPU hot add.

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 the number of CPUs and total memory for the VM.
5) Click **OK**.

9.19.3 Modify Virtual Machine OVF Environment Properties

If a virtual machine includes user-configurable OVF environment properties, you can review and modify those properties. If the vApp containing the virtual machine includes a value for a user-configurable property of the same name, the virtual machine value takes precedence.

Prerequisites

- The virtual machine is powered off and its OVF environment includes user-configurable properties.

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 **Custom Properties** tab, modify the properties and click **OK**.

9.19.4 Configuring Virtual Machine Resource Allocation Settings

Reservation pool vDC 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 VM is provided by the vDC.
- Guarantee that a particular VM is always allocated a higher percentage of the vDC resources than other VMs.
- Set an upper bound on the resources that can be allocated to a VM.

9.19.4.1 Resource Allocation Shares

Shares specify the relative importance of a VM within a vDC. If a VM has twice as many shares of a resource as another VM, it is entitled to consume twice as much of that resource when these two VMs 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 VM.

When you assign shares to a VM, you always specify the priority for that VM relative to other powered-on VMs. The following table shows the default CPU and memory share values for a VM.

Table 9-2. Share Values

Setting	CPU share values	Memory share values
High	2000 shares per virtual CPU	20 shares per megabyte of configured VM memory
Normal	1000 shares per virtual CPU	10 shares per megabyte of configured VM memory
Low	500 shares per virtual CPU	5 shares per megabyte of configured VM memory

For example, a VM 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 VM is powered on. This affects all VMs in the same vDC.

9.19.4.2 Resource Allocation Reservation

A reservation specifies the guaranteed minimum allocation for a VM. The platform will allow you to power on a VM only if there are enough unreserved resources to satisfy the reservation of the VM. The vDC 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 VM 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 VM.

9.19.4.3 Resource Allocation Limit

Limit specifies an upper bound for CPU and memory resources that can be allocated to a virtual machine.

A vDC can allocate more than the reservation to a VM, 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 VM 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 VM 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.

9.19.4.4 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 9.19.4.1 Resource Allocation Shares, 9.19.4.2 Resource Allocation Reservation and 9.19.4.3 Resource Allocation Limit.

Prerequisites

- A reservation pool vDC (this will depend on your billing profile applied to you organisation)

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**.

9.19.5 Modifying Virtual Machine Hard Disks

You can add hard disks, edit hard disks, and delete hard disk from a virtual machine.

9.19.5.1 Add a Virtual Machine Hard Disk

You can add a virtual hard disk to a virtual machine.

Prerequisites

- 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) On the **Hardware** tab, click **Add** in the Hard Disks section.
5) Select the disk size, bus type, bus number, and unit number and click **OK**.

What to do next

Power on the virtual machine and use the guest operating system tools to partition and format the new disk.

9.19.5.2 Edit a Virtual Machine Hard Disk

You can modify the bus number and unit number of a virtual machine hard disk.

Prerequisites

- 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) On the **Hardware** tab, select a new bus number or unit number in the Hard Disks section and click **OK**.

9.19.5.3 Delete a Virtual Machine Hard Disk

You can delete a virtual machine hard disk.

Prerequisites

- 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) On the **Hardware** tab, click **Delete** in the Hard Disks section and click **Yes**.
5) Click **OK**.

9.19.6 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 version 7 and 8 support up to ten NICs.

9.19.6.1 Edit Network Interface Settings

You can disconnect a virtual machine NIC, change the network to which a NIC connects, specify a primary NIC, and change the IP addressing mode for a NIC.

Prerequisites

- 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) In the **NICs** section on the **Hardware** tab, specify 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 other 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.
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**.

9.19.6.2 Reset a Network Interface MAC Address

You can reset a network interface MAC address if, for example, you have a MAC address conflict or if you need to discard saved state quickly and easily.

Prerequisites

- 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 **Hardware** tab.
5) In the **NICs** section, click the **MAC Address** drop-down menu and select **Reset**.
6) Click **OK**.

9.19.6.3 Add a Network Interface

You can add one or more virtual NICs to a virtual machine.

Virtual machines (version 7 and 8) will support up to ten NICs.

For information about supported network adapter types, see the following article at VMware http://kb.vmware.com/kb/1001805.

Prerequisites

- 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) In the **NICs** section on the **Hardware** tab, click **Add**.
5) (Optional) Modify the NIC settings.
6) Click **OK**.

9.19.6.4 Remove a Network Interface

You can remove NICs from a virtual machine.

Prerequisites

- 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) In the **NICs** section on the **Hardware** tab, click **Delete**.
5) Click **OK**.

9.20 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 Web portal.

The platform 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.

9.20.1 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. You must be at least a vApp User.

Prerequisites

- You have created a vApp in which you have 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.

9.20.2 Installing VMware Tools in a vApp

When you install VMware Tools in a virtual machine in a vApp, the process should be understood. 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**. Open the virtual machine console to continue with the installation. For information on installing in a variety of guest OSs, see Table 9-3.

Table 9-3. Installing VMware Tools

Action	Reference
To install on a Windows Guest	9.22.7 Install VMware Tools on a Windows Guest
To install on a Linux Guest	• 9.22.8 Install VMware Tools on a Linux Guest in X with the RPM Installer • 9.22.9 Install VMware Tools on a Linux Guest with the Tar Installer or RPM Installer
To install on a Solaris Guest	9.22.10 Install VMware Tools on a Solaris Guest

If the settings on a guest virtual machine are not in sync with the platform or an attempt to perform guest customization has failed, you can select the virtual machine, right-click, and select **Power on and Force recustomization**.

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 organisation. These options are not used when you use a virtual machine, when you create a new vApp, or add a new virtual machine.

9.20.3 Install VMware Tools in a Virtual Machine in a vApp

vApp deployment can fail if VMware Tools are not installed on the VMs in the vApp.

Prerequisites

- You must stop the vApp.

Procedure

1) 9.22.3.1 Disable Guest Customization
   To install VMware Tools in a virtual machine in a vApp, you must disable guest customization.

2) 9.22.3.2 Start the vApp
   After you install VMware Tools, you must start the vApp.

3) 9.22.3.3 Install VMware Tools
   You must install VMware Tools in your virtual machines to customize the guest operation system.

4) 9.22.3.4 Stop the vApp
   To enable guest customization on a virtual machine, you must stop the vApp.

5) 9.22.3.5 Enable Guest Customization
   After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

6) 9.22.3.6 Start the vApp
   After you install VMware Tools, you must start the vApp.

9.20.3.1 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.

9.20.3.2 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**.

9.20.3.3 Install VMware Tools

You must install VMware Tools in your virtual machines to customize the guest operation system. You are at least a vApp User.

Prerequisites

- Guest customization is disabled 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.

9.20.3.4 Stop the vApp

To enable guest customization on a virtual machine, you must stop the vApp.
You are at least a vApp User.

Prerequisites

- Your vApp is started.

Procedure

1) Click **My Cloud**.
2) Power off your virtual machines.
3) Select a vApp, right-click, and select **Stop**.

The vApp is stopped.

9.20.3.5 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.

9.20.3.6 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**.

9.20.4 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) 9.22.4.1 Save the vApp Template as a vApp
   To install VMware Tools in a vApp, you must save it as a vApp.

2) 9.22.4.2 Disable Guest Customization
   Before you can install VMware Tools on a virtual machine, you must disable guest customization.

3) 9.22.4.3 Install VMware Tools
   You must install VMware Tools in your virtual machines to customize the guest operating system.

4) 9.22.4.4 Enable Guest Customization
   After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

5) 9.22.4.5 Add vApp to Catalog
   After you install or upgrade VMware Tools, you can add the updated vApp to your catalog.

9.20.4.1 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.

9.20.4.2 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**.

9.20.4.3 Install VMware Tools

You must install VMware Tools in your virtual machines to customize the guest operation system. You are at least a vApp User.

Prerequisites
Guest customization is disabled 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.

9.20.4.4 Enable Guest Customization

After you install or upgrade VMware Tools in your VMs, 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.

9.20.4.5 Add vApp to Catalog

After you install or upgrade VMware Tools, you can add the updated vApp to your catalog.

Procedure

1) Select a vApp, right-click, and select **Stop**.
2) Select the vApp, right-click, and select **Add vApp to Catalog**.
3) Select the vApp template, right-click, and select **Properties**.
4) Select **Customize VM Settings** or **Make Identical Copy**.
5) (Optional) Delete the previous version of the vApp template, if necessary.

9.20.5 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) 9.22.5.1 Save the vApp Template as a vApp
   To install VMware Tools in a vApp, you must save it as a vApp.

2) 9.22.5.2 Install or Upgrade VMware Tools
   You can either install VMware Tools or upgrade the current version in your virtual machine.

3) 9.22.5.3 Enable Guest Customization
   After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

4) 9.22.5.4 Add vApp to Catalog
   After you install or upgrade VMware Tools, you can add the updated vApp to your catalog.

9.20.5.1 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.

9.20.5.2 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**.

9.20.5.3 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.

9.20.5.4 Add vApp to Catalog

After you install or upgrade VMware Tools, you can add the updated vApp to your catalog.

Procedure

1) Select a vApp, right-click, and select **Stop**.
2) Select the vApp, right-click, and select **Add vApp to Catalog**.
3) Select the vApp template, right-click, and select **Properties**.
4) Select **Customize VM Settings** or **Make Identical Copy**.
5) (Optional) Delete the previous version of the vApp template, if necessary.

9.20.6 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) 9.22.6.1 Install a New Version of VMware Tools
   After you disable guest customization, you can upgrade VMware Tools.

2) 9.22.6.2 Enable Guest Customization
   After you install or upgrade VMware Tools in your virtual machines, you must enable guest customization.

3) 9.22.6.3 Start the vApp
   After you install VMware Tools, you must start the vApp.

9.20.6.1 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.

9.20.6.2 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.

9.20.6.3 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**.

9.20.7 Install VMware Tools on a Windows Guest

The platform uses VMware Tools to customize the Windows guest operating system.

Prerequisites

- The VMware Remote Console plug-in 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.

9.20.8 Install VMware Tools on a Linux Guest in X with the RPM Installer

You can use an RPM installer to install VMware Tools on a Linux guest operating system.

Prerequisites

- The VMware Remote Console plug-in is 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.
   When VMware Tools is installed, no confirmation or **Finish** button 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 &**.

9.20.9 Install VMware Tools on a Linux Guest with the Tar Installer or RPM Installer

You can use a Tar command or RPM installer to install VMware tools on a Linux guest OS with a Tar or RPM.

Prerequisites

- The VMware Remote Console plug-in is 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-8.5.1-<xxxxxx>.tar.gz** **unmount /dev/cdrom** where <xxxxxx> is the build or revision number of the release.
In the RPM installer	At the command prompt, type **tar zxpf /mnt/cdrom/VMwareTools-8.5.1-<xxxxxx>.i386.gz** **unmount /dev/cdrom** where <xxxxxx> is the build/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 &**.

9.20.10 Install VMware Tools on a Solaris Guest

You can install VMware Tools on a Solaris guest OS.

Prerequisites

- The VMware Remote Console plug-in 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 &**.

9.21 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 9.23.3 Guest Operating System Support, you can see a list of the supported guest operating systems and whether customization is automatic or manual.

9.21.1 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 vDC 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**.

9.21.2 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.

The platform 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, The platform creates a package with guest customization tools. When you deploy and power on the virtual machine for the first time, the platform will copy the package, run the tools, and delete the package from the virtual machine.

9.21.2.1 Understanding Guest Customization

When you customize your guest operating system, there are some settings and options you should know about.

9.21.2.1.1 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. 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 the platform are out of sync with the settings in the guest OS, the **Profile** tab on the virtual machines **Properties** page displays that the settings out of sync with the guest OS and the virtual machine needs guest customization.

9.21.2.1.2 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** checkbox 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 the platform

9.21.2.2 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 9.22 Installing VMware Tools for more information.

9.21.2.3 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.

9.21.2.4 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.

9.21.2.5 Power on and Force Recustomization of a Virtual Machine

If the settings on a guest virtual machine are not in sync with the platform or an attempt to perform guest customization has failed, you can power on and force the recustomization of the virtual machine. You are at least a vApp user.

NOTE: If you select the **Change SID** check box, a SID change will occur on the guest virtual machine.

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 Recustomization**.
4)

The virtual machine is now recustomized.

9.21.2.6 Customize Your Windows NT vApp Template

You must manually customize Windows NT vApp templates.

Prerequisites

- Ensure minimum NT SP6 is installed.
- Ensure VMware Tools are installed.

Procedure

1) Click **Catalogs**.
2) On the **vApp Templates** tab, select a vApp template.
3) Right-click and select **Add to My Cloud**.
4) In the guest OS, shut down the virtual machine.
5) Power off the virtual machine and ensure that the **Enable guest customization** check box is selected.
   You must ensure that the virtual machine's NIC is not set to NONE network.
6) Start the vApp and power on the virtual machine.
   The Customization CD is mounted automatically after the virtual machine powers on.
7) Right-click on the CD ROM and select **Auto play**.
   This step copies the deployPkg.dll file to WINNT folder.

8) Power off the virtual machine.
9) Stop the vApp
10) Right-click the vApp template and select **Copy to Catalog**.
11) (Optional) Delete the original vApp template.

A script starts that copies files to the guest and prepares the virtual machine template for customization.

NOTE If you add new Windows NT vApp Templates, you need to complete only steps 4-7 once. You do not need to repeat these steps for additional virtual machines in the Catalog that result from copying these virtual machines.

9.21.2.7 Customize Your Solaris vApp Template

You must manually customize Solaris vApp templates.

Prerequisites
Ensure VMware Tools are installed.

Procedure

1) Click **Catalogs**.
2) Select a vApp Template, right-click, and select **Add to My Cloud**.
3) In the guest OS, shut down the virtual machine.
4) Ensure that the **Enable guest customization** check box is selected and power off the virtual machine.
5) Start the vApp and power on the virtual machine.
   The Customization CD is mounted automatically after the virtual machine powers on.
6) Log in to the Solaris guest operating system.
7) In the terminal, run these case-sensitive commands:

```
/etc/init.d/volmgt stop
/etc/init.d/volmgt start
sh /cdrom/cdrom/customize-guest.sh install
eject cdrom
```

8) Run **shutdown -y -g0 -i5** to shut down the virtual machine from inside the guest operating system.
9) Stop the vApp.
10) Select the vApp template, right-click, and select **Copy to Catalog**.
11) (Optional) Delete the original vApp template.

A script starts that copies files to the guest and prepares the virtual machine template for customization.

NOTE If you add new Solaris vApp Templates, you need to complete only steps 4-7 once. You do not need to repeat these steps for additional virtual machines in the Catalog that result from copying these virtual machines.

9.21.2.8 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
```

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

4) On the **Guest OS Customization** tab, select the **Enable guest customization** check box.
5) Select the **Allow local administrator password** check box.
6) To force all administrators to change the password at the initial log in, select the **Require administrator to change password on first login** check box. Administrators must know the old password.
7) Determine whether you want an automatically generated password.
   To use a specific password, select **Specify password** and type it.
8) (Optional) To use a specific password, select **Specify password** and type the password.
9) Click **OK**.

The password for your virtual machine is reset.

9.21.2.10 Domain Join Requirements for Windows

The automatic domain join feature has several requirements.

During the customization process, for Windows 2000, Microsoft Sysprep attempts to join the domain before network customization occurs. Therefore, the network properties of the source virtual machine are used to attempt to join the domain.

- If the source virtual machine network properties are such that the domain controller is not resolvable, domain join fails.

- If the source virtual machine was configured with a manually configured DNS, that DNS is contacted to resolve the domain controller even if the manually configured DNS is not on the network. In the case where the DNS cannot be found, domain join fails.

- If the source Windows 2000 virtual machine was configured with DHCP, the new network DHCP is used to attempt to resolve the domain controller. In this case, if the DNS that is configured to the DHCP can resolve the domain controller, domain join succeeds.

During customization for Microsoft Windows XP or later, Microsoft Sysprep resets the guest to configure the network settings to DHCP before attempting to join the domain, regardless of the source virtual machine or network settings. For automatic domain join to succeed, the DHCP on the network must be able to resolve the domain controller.

9.21.2.11 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

- In a virtual machine's **Properties** page, 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 organisation settings is selected by default.
5) Type a domain name, user name, and password.

6) Under **Customization Script**, click **Browse**, to upload a locally saved file.
7) Click **OK**.

The selected virtual machine joins the Windows guest domain.

9.21.3 Guest Operating System Support

The Intelligent Cloud supports a wide variety of 32-bit and 64-bit operating systems in its virtual machine templates and virtual machines. You can only import version 7 and version 8 virtual machines.

9.21.3.1 Microsoft Windows Guest Operating System Support, 32-Bit Support

For 32-bit Windows operating systems, Table 9-4 provides the virtual machine version and whether guest customization is automatic or manual on 32-bit Windows guest OS systems.

Table 9-4. Microsoft Windows Guest Operating System Support, 32-Bit Support

Operating System	Virtual Machine Version	Customization Support
Microsoft Windows 8	Version 9	Automatic
Microsoft Windows 7	Version 9	Automatic
Microsoft Windows Server 2008	Version 9	Automatic
Microsoft Windows Server 2003, Enterprise Edition	Version 9	Automatic
Microsoft Windows Server 2003, Datacenter Edition	Version 9	Automatic
Microsoft Windows Server 2003, Standard Edition	Version 9	Automatic
Microsoft Windows Server 2003, Web Edition	Version 9	Automatic
Microsoft Windows Small Business Server 2003	Version 9	Automatic
Microsoft Windows Vista	Version 9	Automatic
Microsoft Windows XP Professional	Version 9	Automatic
Microsoft Windows 2000 Advanced Server	Version 9	Automatic
Microsoft Windows 2000 Server	Version 9	Automatic
Microsoft Windows 2000 Professional	Version 9	Automatic

9.21.3.2 Microsoft Windows Guest Operating System Support, 64-Bit Support

For 64-bit Windows guest OS, Table 9-5 provides the virtual machine version and whether guest customization is automatic or manual.

Table 9-5. Microsoft Windows Guest Operating System Support, 64-Bit Support

Operating System	Virtual Machine Version	Customization Support
Microsoft Windows 8	Version 9	Automatic
Microsoft Windows 7	Version 9	Automatic
Microsoft Server 2008 R2	Version 9	Automatic
Microsoft Windows Server 2008	Version 9	Automatic
Microsoft Windows Server 2003, Enterprise Edition	Version 9	Automatic
Microsoft Windows Server 2003,Datacenter Edition	Version 9	Automatic
Microsoft Windows Server 2003, Standard Edition	Version 9	Automatic
Microsoft Windows Vista	Version 9	Automatic
Microsoft Windows XP Professional	Version 9	Automatic

9.21.3.3 UNIX/Linux Guest Operating System Support, 32-Bit Support

For 32-bit UNIX and Linux guest OS, Table 9-6 provides the virtual machine version and whether guest
customization is automatic or manual.

Table 9-6. UNIX/Linux Guest Operating System Support, 32-Bit Support

Operating System	**Virtual Machine Version**	**Customization Support**
Red Hat Enterprise Linux 6	Version 9	Automatic
Red Hat Enterprise Linux 5	Version 9	Automatic
Red Hat Enterprise Linux 4	Version 9	Automatic
Red Hat Enterprise Linux 3	Version 9	Automatic
Red Hat Enterprise Linux 2	Version 9	Automatic
SUSE Enterprise Linux 11	Version 9	Automatic
SUSE Enterprise Linux 10	Version 9	Automatic
SUSE Enterprise Linux 8/9	Version 9	Automatic
Open Enterprise Server	Version 9	Automatic
CentOS	Version 9	Automatic
Ubuntu Linux	Version 9	Automatic
Other 2.6x Linux	Version 9	Automatic
Other 2.4x Linux	Version 9	Automatic
Other Linux	Version 9	Automatic

9.21.3.4 UNIX/Linux Guest Operating System Support, 64-Bit Support

For 64-bit UNIX and Linux guest OS support, Table 9-7 provides the virtual machine version and whether guest customization is automatic or manual.

Table 9-7. UNIX/Linux Guest Operating System Support, 64-Bit Support

Operating System	**Virtual Machine Version**	**Customization Support**
Red Hat Enterprise Linux 6	Version 9	Automatic
Red Hat Enterprise Linux 5	Version 9	Automatic
Red Hat Enterprise Linux 4	Version 9	Automatic
Red Hat Enterprise Linux 3	Version 9	Automatic
SUSE Enterprise Linux 11	Version 9	Automatic
SUSE Enterprise Linux 10	Version 9	Automatic
SUSE Enterprise Linux 8/9	Version 9	Automatic
CentOS	Version 9	Automatic
Ubuntu Linux	Version 9	Automatic
Other 2.6x Linux	Version 9	Automatic
Other 2.4x Linux	Version 9	Automatic
Other Linux	Version 9	Automatic

9.21.3.5 Solaris Guest Operating System, 32-Bit Support

For 32-bit Solaris guest OS, Table 9-8 provides the virtual machine version and whether guest customization is automatic or manual.

Table 9-8. Solaris Guest Operating System, 32-Bit Support

Operating System	**Virtual Machine Version**	**Customization Support**
Sun Solaris 11	Version 9	Manual
Sun Solaris 10	Version 9	Manual
Sun Solaris 9	Version 9	Manual
Sun Solaris 8	Version 9	Manual

9.21.3.6 Solaris Guest Operating System, 64-Bit Support

For 64-bit Solaris guest OS, Table 9-9 provides the virtual machine version and whether guest customization is automatic or manual.

Table 9-9. Solaris Guest Operating System, 64-Bit Support

Operating System	Virtual Machine Version	Customization Support
Sun Solaris 11	Version 9	Manual
Sun Solaris 10	Version 9	Manual

10 Appendix A – sample vApp network configurations

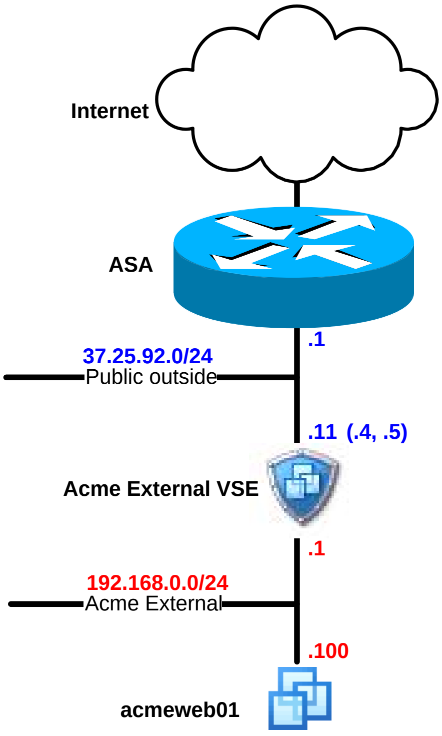
This chapter will describe popular arrangements for vApp networking, leveraging either NAT, firewall, static routing or a combination of all three. References to “VSE” mean the “vShield Edge” device which is at the head of each organistion network or vApp network, and contains the router/firewall.

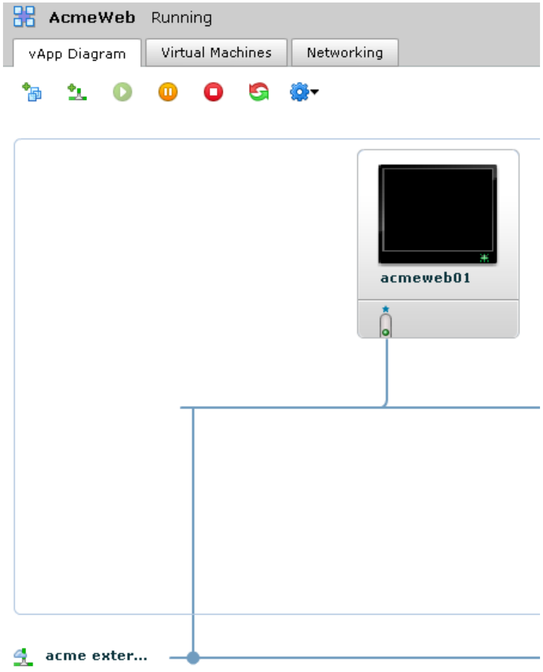
See also:

- 3.2 Managing Organisation Networks
- 8.14 Working with Networks in a vApp

10.1 Web server with IP translation

This is likely the most basic setup. In this example we have one single vApp with a single web server VM in it. The diagram on the left shows the physical connectivity, and the diagram on the right shows this in the vCloud:



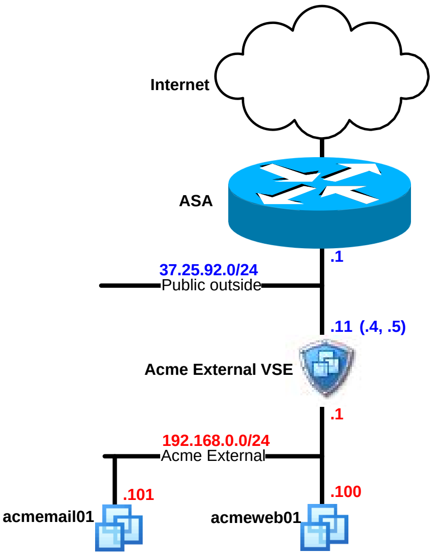


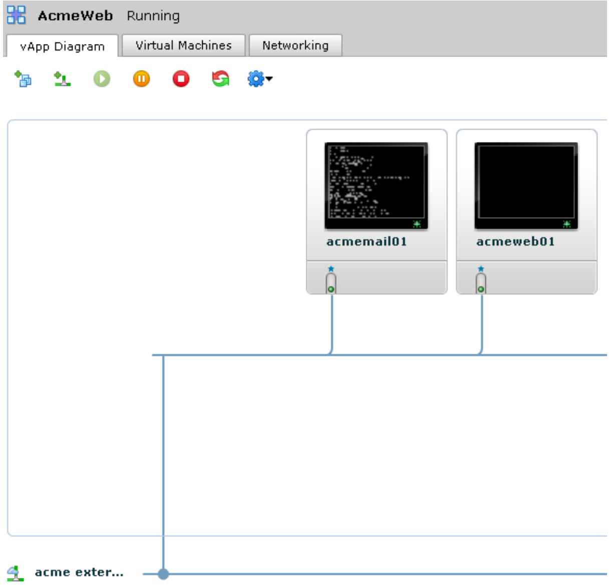
The Acme External VSE is the vShield edge device is the frontend for the organisation in this instance and has two addresses configured for it, (.4 and .5). So that http access is possible to the web server, IP translation is enabled to provide a 1:1 relationship with the inside address, and a firewall rule is added.

Home – Administration – ‘Acme External’ network – Configure Services:
- NAT mapping tab – (applied on External) DNAT from 37.25.92.4:any ANY -> 192.168.0.100:any ANY
- firewall tab – add rule called “http web server” TCP src:any:any dst:37.25.92.4:80

10.2 Web server and mail server using port translation

This setup uses port translation instead of IP translation to enable the use of one public IP address to access two services on disparate VMs in the vApp. The diagram on the left shows the physical connectivity for the two machines, and the diagram on the right shows them in the vCloud.





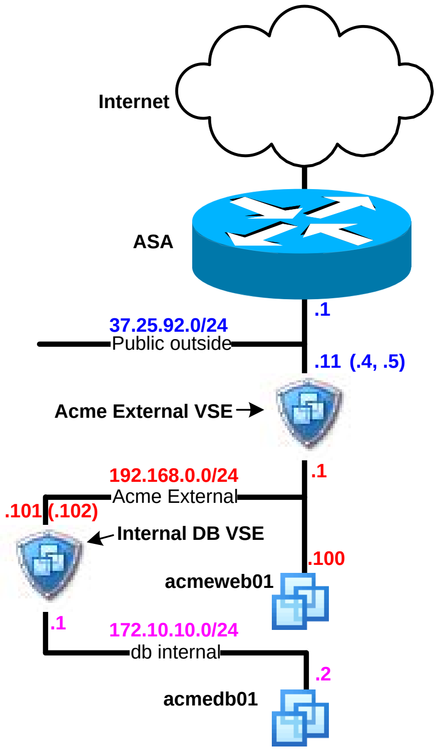
The Acme External VSE is the vShield edge device is the frontend for the organisation in this instance and has two addresses configured for it, (.4 and .5). In this scenario only .4 is to be used, so port translation for port 25 and port 80 are sent to two different inside addresses.

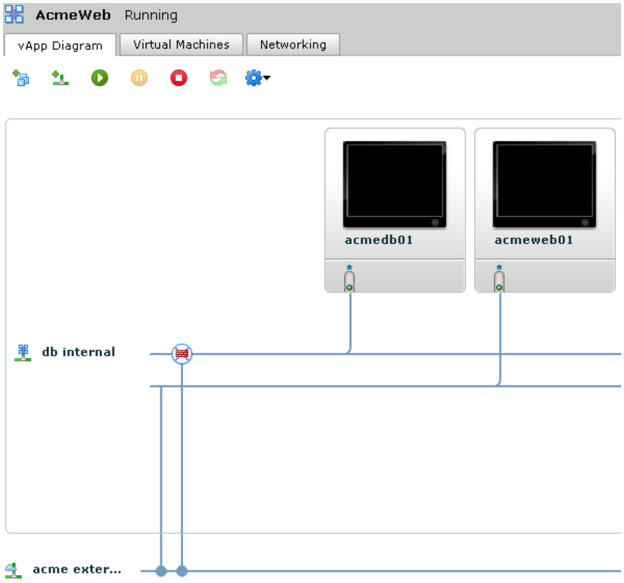
Home – Administration – 'Acme External' network – Configure Services:
- NAT mapping tab – (applied on External) DNAT from 37.25.92.4:25 TCP -> 192.168.0.101:25 TCP
- NAT mapping tab – (applied on External) DNAT from 37.25.92.4:80 TCP -> 192.168.0.100:80 TCP
- firewall tab – add rule called "http web server" TCP src:any:any dst:37.25.92.4:80
- firewall tab – add rule called "smtp mail server" TCP src: any:any dst:37.25.92.4:25

10.3 Web server using IP translation and protected backend DB with IP translation

This setup demonstrates a web server configured in the same manner as in example 1, but has an additional internal vApp network with a database configured in it. This database is able to be accessed from the External network by way of a NAT'd address. This can provide a more secure way of hiding the database further down in the vApp and setting firewall rules accordingly.

The diagram on the left shows the physical connectivity for this vApp and the diagram on the right shows this as it would look in vCloud:





The Acme External VSE is the vShield edge device is the frontend for the organisation in this instance and has two addresses configured for it, (.4 and .5). So that http access is possible to the web server, IP translation is enabled to provide a 1:1 relationship with the inside address, and a firewall rule is added.

Home – Administration – 'Acme External' network – Configure Services:
- NAT mapping tab – (applied on External) DNAT from 37.25.92.4:any ANY -> 192.168.0.100:any ANY
- firewall tab – add a firewall rule called "http web server" TCP src:any:any dst:37.25.92.4:80

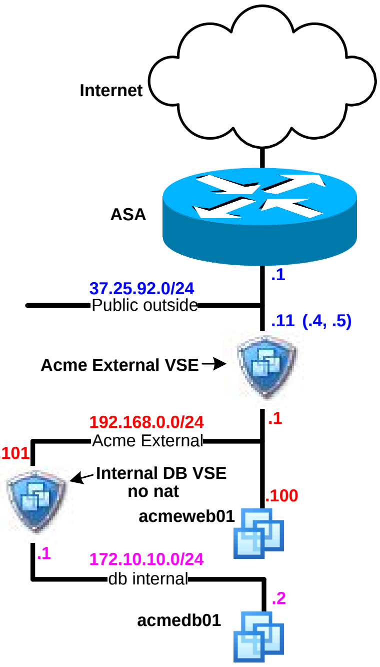
The Internal DB VSE is an internal vApp vShield Edge and this alike the external network has IP translation applied. There is a 1:1 relationship with the external address 192.168.0.102 that maps to 172.10.10.2 which is the database server. A firewall is applied on this VSE to allow the web server to connect to it. (note, to access 'Configure Services' for the below, tick the box labelled "Show networking details" under the networking tab for the vApp.

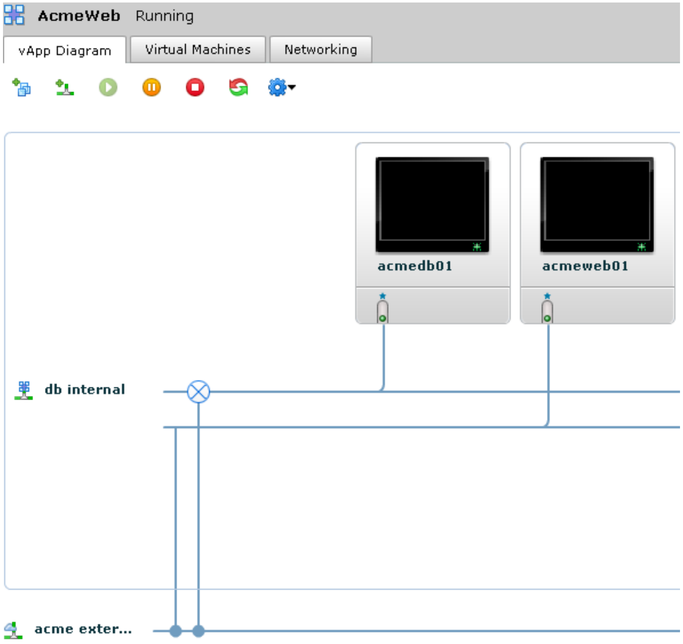
My Cloud – vApps –'AcmeWeb' vApp – Networking – db Internal - Configure Services:
- NAT mapping tab – IP Translation from 192.168.0.102 -> 172.10.10.2 THIS IS AUTOMATICALLY APPLIED
- firewall tab – add rule called "mysql db server" inbound TCP src:192.168.0.100:* dst:192.168.0.102:3306

10.4 Web server using IP translation and protected backend DB with no NAT

This setup demonstrates a similar configuration to that of example 3, but this time the db internal network VSE has NAT disabled. This time the web server will have to connect to the INSIDE address of the db server, so has to connect to it via a static route. This static route needs to be applied inside the guest. A better way of doing this is shown in example 5, where the web server is on its own internal network as well. The static route can then be applied to the web servers internal network and vice versa.

The diagram on the left shows the physical connectivity for this vApp and the diagram on the right shows this as it would look in vCloud:





The Acme External VSE is the vShield edge device is the frontend for the organisation in this instance and has two addresses configured for it, (.4 and .5). So that http access is possible to the web server, IP translation is enabled to provide a 1:1 relationship with the inside address, and a firewall rule is added.

Home – Administration – 'Acme External' network – Configure Services:
- NAT mapping tab – (applied on External) DNAT from 37.25.92.4:any ANY -> 192.168.0.100:any ANY
- firewall tab – add a firewall rule called "http web server" TCP src:any:any dst:37.25.92.4:80

The Internal DB VSE is an internal vApp vShield Edge but has no NAT. In this example the firewall is also disabled showing (the db server will have no access to the Internet being that there is no nat).

My Cloud – vApps –'AcmeWeb' vApp – Networking – db Internal - Configure Services:
- NAT mapping tab – none
- firewall tab – disabled

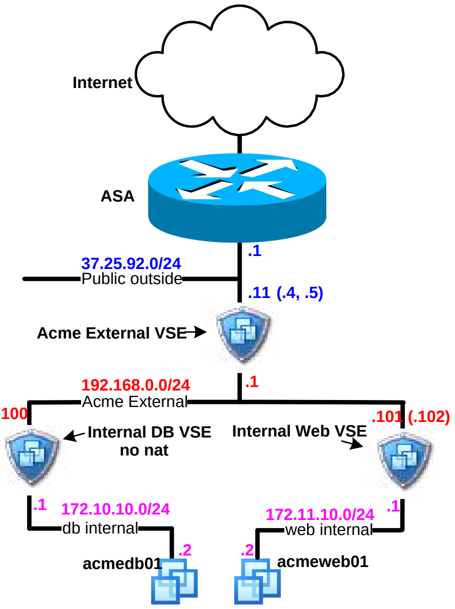
The web server will require a static route in this instance. It is a Linux machine so the following command will need to be run:

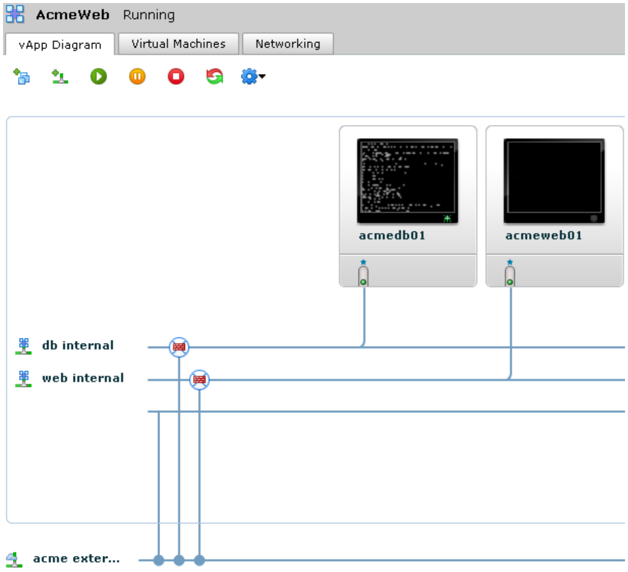
```
- route add -net 172.10.10.0 netmask 255.255.255.0 gw 192.168.0.101
```

10.5 Web server and protected DB in internal networks

This setup is a better configuration than example 4 and demonstrates that NAT can be performed twice. The web server in this instance is in a second vApp network that we have created, so the translation from the public side will be 37.25.92.4 -> 192.168.0.102 -> 172.9.10.2. Note that each VSE on the internal vApp networks this time has a static route to each other vApp network.

The diagram on the left shows the physical connectivity for this vApp and the diagram on the right shows this as it would look in vCloud:





The Acme External VSE is the vShield edge device is the frontend for the organisation in this instance and has two addresses configured for it, (.4 and .5). So that http access is possible to the web server, IP translation is enabled to provide a 1:1 relationship with the inside address that appears on the front of the web internal VSE, and a firewall rule is added.

Home – Administration – ‘Acme External’ network – Configure Services:
- NAT mapping tab – (applied on External) DNAT from 37.25.92.4:any ANY -> 192.168.0.100:any ANY
- firewall tab – add a firewall rule called “http web server” TCP src:any:any dst:37.25.92.4:80

The web internal VSE is an internal vApp vShield Edge and has NAT enabled. We check the translation to the inside web server, add a firewall rule and setup static routing to the db internal network.

My Cloud – vApps –‘AcmeWeb’ vApp – Networking – web internal - Configure Services:
- NAT mapping tab – ip translation from 192.168.0.102 -> 172.11.10.2 THIS IS AUTOMATICALLY APPLIED
- firewall tab – add a firewall rule called “http acmeweb” TCP src:*:* dst:192.168.0.102:80
- static routing – 172.10.10.0/24 via 192.168.0.100

The db internal VSE is an internal vApp vShield Edge and has NAT disabled, but we have the firewall on this time. We add a firewall rule and setup static routing to the web internal network. Note the db inbound firewall rule references the outside translated address for the web server.

My Cloud – vApps –‘AcmeWeb’ vApp – Networking – db internal - Configure Services:
- NAT mapping tab - disabled
- firewall tab – add a firewall rule called “web to db” TCP src:192.168.0.102:* dst:172.10.10.2:3306
- static routing – 172.11.10.0/24 via 192.168.0.101

11 Appendix B – Backup and Restore

If the option to have your virtual machines backed up in the vCloud platform, restores are performed administratively on request by MT.

11.1 Restorations of VMs

Once MT has received instruction to restore a VM, we will restore the machine to a new vApp (using a new name) into your vDC. There are several choices to be able to access the data within the restored VM.

Depending on what needs to be done, i.e. if the original machine is irreparable, or a single file or set of files needs to be obtained, these are the following choices:

1) 11.1.1 Replace original machine with the restored version (where the restored VM is present in a new vApp)
2) 11.1.2 Reconfigure the restored VM and access it from the outside world by configuring a unique address on the external network and use port translation / ip translation from a public IP address.
3) 11.1.3 Reconfigure the VM and access it as an adjacent machine, for example from the original machine by configuring a unique address on the external network (or adding a separate internal network on both original and restored VMs)

11.1.1 Replace original machine with the restored version

1) Login and navigate to the **My Cloud** tab, and select the original vApp. Click on the **Virtual Machines** tab and Right click on the original VM and select properties. Establish the details for
   a. VM Name (found under the **General** tab)
   b. Computer Name (found under the **General** tab, this is likely the same as the virtual machine name unless it has been updated in the guest OS)
   c. VM description (found under the **General** tab)
   d. VM connected networks (and their order), and the IP addresses. (found under the **Hardware** tab)
   e. Guest Customization properties including, **Allow local administrator access** and associated password configuration, and any other properties if required. (Found under the **Guest Customization** tab).

2) The original VM can now be safely discarded provided it is powered off. Note that this will PERMANENTLY delete the original VM. Right click the original VM under the Virtual Machines tab and click **Yes** once prompted to delete it.

3) Navigate back to the **My Cloud** tab, select the new vApp, click on the **Virtual Machines** tab Right click on the restored VM and select **Move To…**

4) Locate the original vApp to move the restored VM to and click **Next**

5) It is best to leave the settings as default here, as the VM's properties will be updated from step 9 later in this procedure. Click **Next** and **Finish** to continue, this will then clone the VM to the original vApp, and remove the restored VM.

6) Once this is completed, the new vApp will be empty, it is now safe to remove the temporary vApp from the **My Cloud** tab and clicking vApps on the left, right clicking on the empty vApp and selecting **Delete**, and clicking on **Yes**.

7) Right click on the restored VM and select properties

8) Place the correct name and description under the **General** tab

9) Add the required networks under the hardware tab (being careful to note the order). There is a possibility that a new IP address will be statically assigned if the default **Static IP Pool** option is selected for the network adapters. It is suggested that **Static Manual** be chosen and the original IP addresses are entered for the respective network adapters.

10) Ensure that guest customisation is enabled under the **Guest OS Customization** tab and the required admin access and password is set the same as the original machine.

    CAUTION: for a direct replacement of a windows machine it will usually not be required to change the SID as this is normally for deploying multiple copies of a single template. As this scenario is describing a replacement and the restored VM contains the old SID, this option should NOT be selected. For Linux machines this setting has no affect.

11) Once all done press OK, and power on the machine. If the machine is windows, a reboot will occur on first boot to enable the guest customisation. If it is Linux, the guest customisation is run at boot-time.

11.1.2 Reconfigure the restored VM and access it from the outside world

1) Login and navigate to the **My Cloud** tab, and select the vApp that contains the restored VM. Click on the **Virtual Machines** tab and Right click on the restored VM and select properties.

2) Under the **Hardware** tab, connect NIC0 to the external network

3) Right click on the restored VM and select properties

4) Ensure that guest customisation is enabled under the **Guest OS Customization** tab and the required admin access and password is set the same as the original machine. As this is an adjacent machine, if the machine is windows, the SID should be changed as well to prevent a machine ID conflict.

5) Once done, press OK

6) After a brief wait, the inside IP address will now be visible for this machine on the external organisation network. Make a note of this address.

7) On the organisation network use either port or IP NAT translation (see 3.2.1.6 Add a Port Forwarding Rule to an Organisation Network or 3.2.1.7 Add an IP Translation Rule to an Organisation Network), create a mapping and firewall rule to enable remote access to this machine to connect to it from the outside world. (See 3.2.1.3 Add a Firewall Rule to an Organisation Network). If it is a Linux machine, you will likely need to use SSH (TCP port 22), if it windows, you will likely need to use RDP (TCP port 3389).

11.1.3 Reconfigure the restored VM and access it from an adjacent machine

1) Login and navigate to the **My Cloud** tab, and select the vApp that contains the restored VM. Click on the **Virtual Machines** tab and Right click on the restored VM

and select properties.

2) Under the **Hardware** tab, connect NIC0 to the external organisation network

3) Right click on the restored VM and select properties

4) Ensure that guest customisation is enabled under the **Guest OS Customization** tab and the required admin access and password is set the same as the original machine. As this is an adjacent machine, if the machine is windows, the SID should be changed as well to prevent a machine ID conflict.

5) Once done, press OK

6) After a brief wait the inside IP address will now be visible for this machine on the external network. Make a note of this address.

7) Power on the restored machine

8) Provided that an adjacent machine is present on the same organisation network, it should now be possible to connect to the restored virtual machine using the address discovered in step 6.

12 Version history

1.0.0 first release for v1.5 28/03/12

1.0.1 minor corrections 03/04/12

1.0.2 minor corrections 20/04/12

5.1.0 second release with updates for vCloud 5.1 with vCNS 5.1.2

5.1.2 second release with updates for vCloud 5.1.2 with vCNS 5.1.2b and various updates