Installing and Configuring vCloud Connector

vCloud Connector 2.5.0

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

EN-001127-02

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

Copyright © 2011–2013 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at http://www.vmware.com/go/patents.

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

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

Contents

Installing and Configuring vCloud Connector

Installing and Configuring vCloud Connector provides a brief overview of VMware vCloud ® Connector™. It also provides detailed information on installing and configuring vCloud Connector server and vCloud Connector nodes and setting up the vCloud Connector UI .

Intended Audience

This information is intended for anyone who wants to set up vCloud Connector. You should be familiar with VMware vSphere® Client™, VMware vCloud Director®, and deploying virtual appliances.

1 vCloud Connector Editions

vCloud Connector 2.5 has two editions: VMware vCloud® Connector™ 2.5 Core and VMware vCloud® Connector™ 2.5 Advanced.

vCloud Connector 2.5 Advanced requires a valid VMware vCloud® Suite 5.1 or 5.5 license key to enable its features. In addition to vCloud Connector 2.5 Core features, it includes these advanced features.

- Content Sync
- Stretch Deploy (also referred to as Datacenter Extension)

See Chapter 4, "Entering the License Key for vCloud Connector Advanced Edition," on page 53 for information on how to assign the license key.

vCloud Connector Overview 2

This section provides an overview of vCloud Connector. It describes the functionality of vCloud Connector and the components that make it up.

This chapter includes the following topics:

vCloud Connector

vCloud Connector is an enterprise product that provides a single user interface for overseeing multiple public and private clouds and for transferring cloud content from one cloud to another. It allows you to connect multiple clouds, both internal and external, in a single user interface.

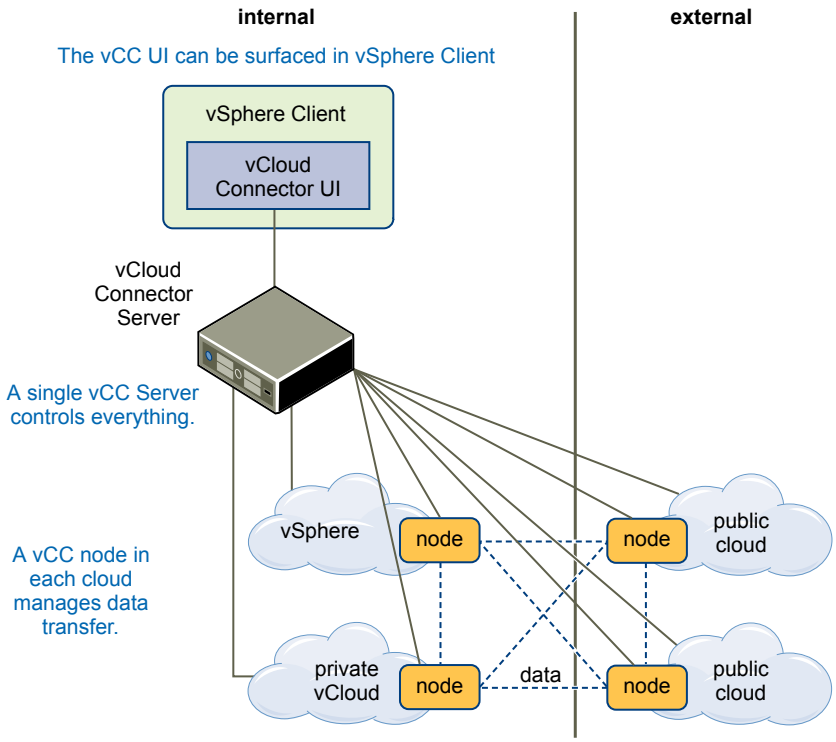
Using vCloud Connector, you can stop and start virtual machines, check their performance, and transfer virtual machines, vApps, and templates from one cloud to another.

Using vCloud Connector Advanced edition, you can also extend your private datacenter to a public vCloud with Datacenter Extension and set up a Content Library to distribute and synchronize templates across clouds.

vCloud Connector Components

vCloud Connector consists of three distinct components: the vCloud Connector UI, the vCloud Connector server, and vCloud Connector nodes.

Figure 2-1. vCloud Connector Components



vCloud Connector UI

vCloud Connector UI is the user interface that the vCloud Connector server produces. It can be surfaced in vSphere Client. You decide where to display the UI during the configuration process.

vCloud Connector Server

The vCloud Connector server is a virtual appliance that coordinates the activity of vCloud Connector, controls vCloud Connector nodes, and produces the vCloud Connector UI. Only one vCloud Connector server is needed.

vCloud Connector Nodes

vCloud Connector nodes are virtual appliances that handle transferring content from one cloud to another. A vCloud Connector node must be installed in every vSphere or vCloud Director-based cloud that vCloud Connector oversees.

On public clouds, the service provider installs a vCloud Connector node as a multi-tenant node for multiple customers to use.

Planning Your vCloud Connector Installation

Before you install vCloud Connector, you need to do some basic high-level planning.

You need to decide the following.

- Where you want to install the vCloud Connector server
- Which clouds you want to be able to add to the vCloud Connector UI. You must install a vCloud Connector node in each cloud that you want to add.

On vCloud Director clouds, you do not need to install a node for each organization. vCloud Connector nodes are multi-tenant, that is, one node can be used by multiple organizations to transfer content to and from the cloud. If you are a public vCloud service provider or the system administrator of a private vCloud Director cloud, you can choose to install one node in the cloud for multiple organizations to use.

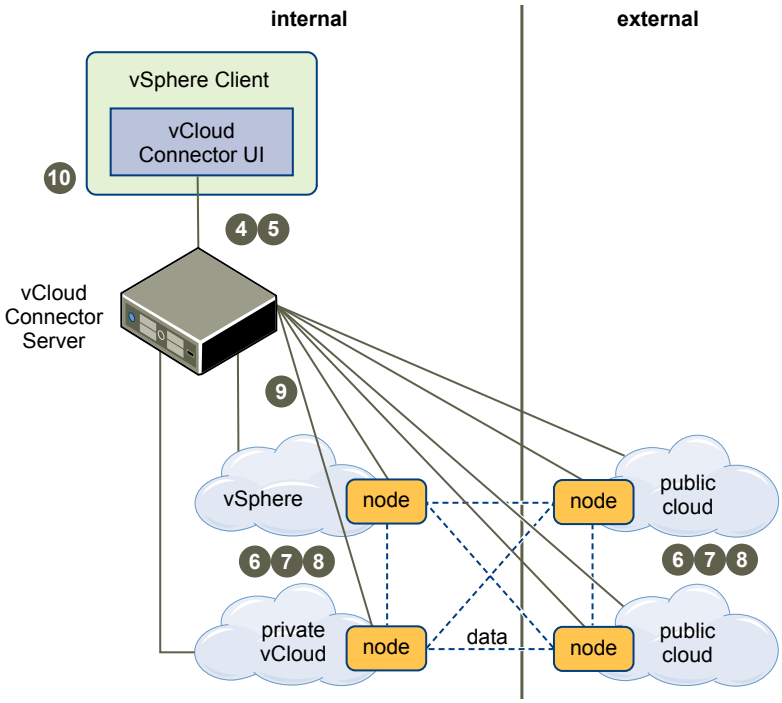
- In which vSphere Client you want to surface the UI

You also need to collect specific information to use during the installation and configuration process. What you need to know depends on your specific installation decisions. A detailed description of the information you should collect is covered in "Collect Necessary Information," on page 14.

Installing vCloud Connector 3

Installing vCloud Connector is a multi-step process. This section gives you a high-level overview of the steps you need to take.

Figure 3-1. vCloud Connector Installation and Configuration Workflow



You install a vCloud Connector node in each cloud that you want to connect. To connect a public cloud, you can either install your own node in the cloud or ask your service provider to install a multi-tenant node. You only need one vCloud Connector server.

This figure illustrates all the combinations that you can set up with vCloud Connector. Typically, you use a subset of these. Common installation scenarios include using vCloud Connector to connect the following.

- Connect a private vSphere cloud with a public vCloud.
- Connect a private vCloud Director cloud with a public vCloud.
- Connect a private vSphere cloud with a private vSphere cloud.
- Connect a private vCloud Director cloud with a private vCloud Director cloud.
- Connect a private vSphere cloud with a private vCloud Director cloud.

Procedure

1 Collect Necessary Information on page 14

Print this worksheet section to help you collect the information you need to install and configure vCloud Connector.

2 Check System Requirements on page 16

You must ensure that your system meets the minimum requirements before you install vCloud Connector.

3 Download the vCloud Connector Virtual Appliances on page 18

The vCloud Connector server and vCloud Connector node are packaged as virtual appliances. You download the virtual appliances from the vCloud Connector Download page.

4 Install vCloud Connector Server on page 18

You can install a vCloud Connector server in a vSphere cloud or in a vCloud Director cloud.

5 Configure vCloud Connector Server on page 29

You use the vCloud Connector server Admin Web console to do basic configuration tasks, such as defining your time zone, specifying proxy servers, or setting log levels. What you need to do depends on your particular installation.

6 Install vCloud Connector Nodes on page 32

You can install vCloud Connector nodes in vSphere or vCloud Director clouds.

7 Register vCloud Connector Nodes with Clouds on page 43

After you install a vCloud Connector node for a cloud, you need to associate it with the cloud.

8 Configure vCloud Connector Nodes on page 44

You use the vCloud Connector node Admin Web console for each of your nodes to perform basic configuration tasks, such as defining your time zone, specifying proxy servers, or setting log levels. What you need to do depends on your particular installation.

9 Register vCloud Connector Nodes with vCloud Connector Server on page 49

You use the vCloud Connector server Admin Web console to register vCloud Connector nodes with the vCloud Connector server. The nodes can be installed on vSphere, private vCloud Director clouds, or public vClouds. The registration allows the server to manage the nodes.

10 Register the vCloud Connector UI on page 50

To use the vCloud Connector UI, you register it to a vSphere Client.

Collect Necessary Information

Print this worksheet section to help you collect the information you need to install and configure vCloud Connector.

Accounts

You need the following accounts.

Table 3-1. Account Information

Account Type	Information Needed	Used For
A My Vmware™ account. You can get an account from www.vmware.com.	User name and password	Downloading vCloud Connector
One of the following: ■ VMware® vCenter Server™ administrator account ■ VMware vCloud Director® account with at least organization administrator status	User name, password, and URL or IP address for the appropriate entity	Installing vCloud Connector server
vCenter Server administrator account for each vSphere cloud	User name, password, and URL or IP address	Installing vCloud Connector node
vCloud Director account with at least organization administrator status for each vCloud Director cloud	User name, password, and URL or IP address	Installing vCloud Connector node

Proxy Servers

You need the following proxy information.

Table 3-2. Proxy Information

Install Type	Information Needed	Condition
vCloud Connector server	host:port	If the server needs a proxy to be able to access systems beyond the firewall in the location in which it is installed.
vCloud Connector node - per node	host:port	If the node needs a proxy to be able to access systems beyond the firewall in the location in which it is installed.

NOTE UDT-based data transfer in vCloud Connector is only compatible with SOCKS5-compliant proxy servers, as these proxy servers support the UDP protocol. You cannot use UDT-based data transfer with any other types of proxy servers.

Network

If you are using a static IP address (and not DHCP) for your vCloud Connector server or vCloud Connector node, you need the following information for each instance.

Table 3-3. Network Information

Network Information
An available static IP address
The netmask for that address
The IP address of the gateway

Table 3-3. Network Information (Continued)

Network Information
The IP address of a primary and secondary DNS server
A host name (optional)

For information on network paths in data transfers, see Chapter 9, "Cross-Cloud Data Transfer and Network Connectivity," on page 79.

Displaying the vCloud Connector UI

To set up the vCloud Connector UI in a VMware vSphere® Client™, you need the following information.

Table 3-4. vCloud Connector UI in vSphere

vCloud Connector UI in vSphere
The IP address or fully qualified domain name of the vCenter Server to which you will be connecting.
A user name and password for the vCenter Server.
The IP address or fully qualified domain name of the deployed vCloud Connector server. This information is assigned when the vCloud Connector server is first deployed.

Check System Requirements

You must ensure that your system meets the minimum requirements before you install vCloud Connector.

Product Requirements

To install and configure a vCloud Connector server and nodes, you need to install the following VMware products.

Table 3-5. VMware Products

Product	Supported Version	Notes
vSphere	4.0, 4.1, 5.0, 5.1, 5.5	Required if you are deploying the vCloud Connector server or vCloud Connector nodes on vSphere. NOTE To use the Stretch Deploy feature (Datacenter Extension), you must install vSphere 5.1 or later.
vCloud Director	1.5, 5.1, 5.5	Required if you are deploying the vCloud Connector server or vCloud Connector nodes on vCloud Director. NOTE To use the Stretch Deploy feature (Datacenter Extension), you must install vCloud Director 5.1 or later.

Table 3-5. VMware Products (Continued)

Product	Supported Version	Notes
vShield Manager	5.1.2, 5.5	Required for the Stretch Deploy feature (Datacenter Extension) only.
vSphere Client	4.0, 4.1, 5.0, 5.1, 5.5	Required as the vCloud Connector UI is registered as a plug-in in vSphere Client.

NOTE The Stretch Deploy feature has special system requirements. See System Requirements for Stretch Deploy in *Using vCloud Connector* for more information.

Supported Browsers

To access the vCloud Connector server and node Admin Web consoles, you need a browser.

Table 3-6. Supported Browsers

Browser	Supported Version
Internet Explorer	8, 9
Firefox	15, 16
Chrome	22, 23

The browser must be set to accept third-party cookies.

NOTE Do not use Firefox to log in to the vCloud Connector server or node Admin Web console. Some tabs, such as the Server tab in the server Admin Web console and the Node tab in the node Admin Web console, display blank pages on Firefox.

Required Ports

vCloud Connector uses the following ports to communicate between its various components: server, nodes, and the server and node Admin Web consoles.

Table 3-7. Port Information

Port Number	Use
443	Used when SSL is enabled. This port is used for communication between the vCloud Connector server and vCloud Connector nodes and between nodes.
80	Used when SSL is disabled. This port is used for communication between the vCloud Connector server and vCloud Connector nodes and between nodes.
8190	Required on the destination node for UDT-based data transfer. NOTE When you copy data between a private cloud and a public cloud, port 8190 needs to be open on the public cloud.
5480	This port is used for communication with the vCC server and vCC node Admin Web consoles.

NOTE Ports 80 and 443 are also used for the Local Content Directory node, which is a node that is automatically installed with the vCloud Connector server and used for the Content Library. Port 80 is used when SSL is disabled and port 443 is used when SSL is enabled.

Download the vCloud Connector Virtual Appliances

The vCloud Connector server and vCloud Connector node are packaged as virtual appliances. You download the virtual appliances from the vCloud Connector Download page.

Prerequisites

You have collected the information specified in "Collect Necessary Information," on page 14.

Procedure

1 Go to the vCloud Connector Download page.

2 Click **Download**.

3 Scroll down to the **Product Downloads** section and download both the `vCCServer` and `vCCNode` files.

   a Click either **Download Manager** or **Manually Download**.

   For information about each method, click the **Need help downloading?** link at the top of the section.

   b Log in with your My VMware™ account information.

   c Read and accept the End User License Agreement.

   A dialog box appears that prompts you to open or save the zip file.

   d Download the zip file to your desktop.

4 In separate directories, unzip the vCloud Connector server and vCloud Connector node virtual appliance zip files.

Install vCloud Connector Server

You can install a vCloud Connector server in a vSphere cloud or in a vCloud Director cloud.

Only one vCloud Connector server is required for each vCloud Connector installation. Choose one of the following options to install your server.

Install vCloud Connector Server in vSphere

You can install a vCloud Connector server in vSphere.

For information on installing vCloud Connector in a Linked Mode vCenter server configuration, see "Installing vCloud Connector in Linked Mode vCenter Server Configurations," on page 19.

Prerequisites

You must have an administrator account for the vSphere instance in which you deploy the vCloud Connector server. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 18.

Procedure

1 Log in to vSphere Client.

2 Select **File > Deploy OVF template**.

3 Click **Browse** and navigate to the OVF directory of the server zip file you downloaded.

4 Click **Next**.

5 Proceed through the wizard.

You can either use the Networking Properties step in the wizard to set basic network properties or you can wait and set those properties when you configure your server.

NOTE If you are going to use a static IP address, you need to assign it here. Proxy information is set during "Configure vCloud Connector Server," on page 29.

6 In the vSphere Client, select **Inventory > VMs and Templates** to see the virtual machine that is created.

7 Right-click the virtual machine and select **Power > Power on** to power it on.

8 Click the **Summary** tab and find the vCloud Connector server's IP address in the **General** section. The **IP address** field (not the **Host** field) displays the IP address of the vCloud Connector server. Make a note of the IP address. You will need it later in the process.

Installing vCloud Connector in Linked Mode vCenter Server Configurations

vCloud Connector is compatible with Linked Mode vCenter server configurations. You install a vCloud Connector server or vCloud Connector nodes in vCenter server instances in a Linked Mode configuration in the same way that you install them on single vCenter server instances.

For information about Linked Mode vCenter server configurations, see the VMware vSphere Documentation Center.

Installing a vCloud Connector Server in a Linked Mode vCenter Server Configuration

You install one vCloud Connector server. You can install it in any of the vCenter server instances in the Linked Mode configuration.

Installing vCloud Connector Nodes in a Linked Mode vCenter Server Configuration

You install a vCloud Connector node for each vCenter server instance that you want to manage in vCloud Connector. You then register each node with your vCloud Connector server.

Registering the vCloud Connector UI with a vSphere Client Associated with a Linked Mode vCenter Server Configuration

The vCloud Connector UI appears as a plug-in in vSphere Client. You can register the vCloud Connector UI to any of the vCenter server instances in the Linked Mode configuration.

When you register the vCloud Connector UI, specify the IP address or URL of any of the vCenter server instances. The UI appears in the vSphere Client for all the vCenter instances.

NOTE If the plug-in does not appear in vSphere Client, clear the Internet Explorer cache, then close and restart vSphere Client.

Install vCloud Connector Server in vCloud Director 1.5

You can install a vCloud Connector server in vCloud Director 1.5.

NOTE If you install a vCloud Connector server in a public cloud, you can only connect to public clouds in your vCloud Connector UI.

Prerequisites

You must have at least organization administrator access in the vCloud Director cloud in which you install the vCloud Connector server.

Procedure

1 Add vCloud Connector Server to a vCloud Director 1.5 Catalog as a vApp Template on page 20

Before you can deploy a vCloud Connector server in a vCloud Director 1.5 cloud, you must upload the virtual appliance to a catalog as a vApp template. You do not need to upload an additional template if a template is already uploaded to a master catalog that multiple organizations share.

2 Create the vCloud Connector Server from the Template in a vCloud Director 1.5 Cloud on page 21

After the vCloud Connector server is added to the vCloud Director 1.5 cloud as a template, you can use it to create a running instance on that cloud.

3 Set Up NAT Mapping for vCloud Connector Server in vCloud Director 1.5 on page 22

If you select a NAT-based network connection when you deploy your vCloud Connector server, you need to set up NAT mapping and firewall rules.

Add vCloud Connector Server to a vCloud Director 1.5 Catalog as a vApp Template

Before you can deploy a vCloud Connector server in a vCloud Director 1.5 cloud, you must upload the virtual appliance to a catalog as a vApp template. You do not need to upload an additional template if a template is already uploaded to a master catalog that multiple organizations share.

Prerequisites

You must have system administrator or organization administrator access in the vCloud Director cloud in which you install the vCloud Connector server. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 18.

Procedure

1 Log in to the vCloud Director Web console using a supported browser.

2 Click **Catalogs**.

If you log in as system administrator, select your organization first, then click the **Catalogs** tab.

3 Double-click the catalog to which you want to upload the vCloud Connector server, then click the **vApp Templates** tab.

4 Click the **Upload** icon.

5 In the Upload OVF package as a vApp Template dialog box, click **Browse**, accept the security certificate if you are prompted to do so, and select the vCloud Connector server OVF file that you downloaded.

6 Specify a name and, optionally, a description, for the vApp template.

7 Select the virtual datacenter and catalog for the template.

8 Click **Upload**.

The upload process begins. You can monitor the status of the upload in the **Transfer Progress** popup.

NOTE It may take several seconds after the upload itself has finished for the process to be finalized in the cloud.

Create the vCloud Connector Server from the Template in a vCloud Director 1.5 Cloud

After the vCloud Connector server is added to the vCloud Director 1.5 cloud as a template, you can use it to create a running instance on that cloud.

Prerequisites

You must have at least organization administrator access in the vCloud Director cloud in which you install the vCloud Connector server.

Procedure

1 On the **vApp Templates** tab of the catalog to which you uploaded, right-click the name of your vCloud Connector server template and select **Add to My Cloud**.

The Add to My Cloud popup appears.

2 Give the server vApp an easily identifiable name and provide a description.

3 Set the leases for the server vApp and click **Next.**

4 Read and accept the EULA, and click **Next**.

5 Select an appropriate network from the **Network** drop-down menu.

Unless all your vCloud Connector nodes and the vCloud Connector server are behind the same firewall, you must select a network that is configured to access the Internet. Ask your service provider or network administrator for more information.

NOTE If your provider uses NAT, you will need to set up NAT mapping after your server is deployed. See "Set Up NAT Mapping for vCloud Connector Server in vCloud Director 1.5," on page 22.

---

6 Select the appropriate IP Assignment from the drop-down menu and click **Next**.

If there is a static IP pool, that is probably a reasonable choice. Ask your service provider or network administrator for more information.

7 In the Networking Properties page, use the information you collected before you began installing vCloud Connector to specify the DNS server, IP address, Netmask, and Default Gateway. If you are using DHCP, leave the fields blank.

8 In the Configure Networking page, leave both check boxes unselected, and click **Next**.

9 In the Ready to Complete page, review the settings and click **Finish**.

10 Click the **My Cloud** tab, then select **vApps** in the My Cloud panel.

You see the vApp being created.

11 In the My Cloud panel, select **VMs**, right-click your vCloud Connector server, and select **Properties**.

12 In the Virtual Machine Properties window, click the **Guest OS Customization** tab.

13 Select **Enable guest customization**, then click **OK**.

14 In the My Cloud panel, select **vApps**, then right-click the console icon of the vCloud Connector server and select **Start**.

15 When the server on vCloud Director 1.5 is in running state, click **VMs** in the My Clouds panel and make a note of the IP address of the server VM.

You need the IP address later in the registration process.

Set Up NAT Mapping for vCloud Connector Server in vCloud Director 1.5

If you select a NAT-based network connection when you deploy your vCloud Connector server, you need to set up NAT mapping and firewall rules.

There are multiple approaches to managing this issue. Decide whether you wish to use NAT to forward only the ports necessary for vCloud Connector operation or to forward all ports and then set up a firewall rule to filter all but the required ports. See "Check System Requirements," on page 16 for the list of required ports.

Prerequisites

Your appliance is deployed and you are logged in to the vCloud Director Web console as organization administrator or system administrator.

Procedure

1 Click the **Administration** tab and select **Networks** in the left panel.

2 Find the network you are using in the Networks list, right-click, and select **Configure Services**.

3 In the Configure Services dialog box, click the **NAT Mapping** tab and click **Add** at the bottom of the popup to create the NAT rule.

   The Add NAT Rule popup appears.

4 Select one of the External IP addresses from the drop-down menu.

   Note this address if you plan to set up a firewall rule.

5 If you wish to NAT all ports, enter * for the first port entry.

   If you wish to NAT only the required ports, create a rule for each port.

6 Enter the internal IP address from your initial setup and match the port entry for this rule.

7 Click **OK** and click **OK** again.

8 If you are using a firewall rule to control traffic, click the **Firewall** tab and select the **Enable firewall** check box.

9 Click **Add** at the bottom of the pop-up menu to create a new firewall rule.

   Create a rule for each necessary port.

   The Add Firewall Rule popup appears.

10 Give the rule a name and select the **Incoming** option.

11 Type the source IP address and the source port.

   For incoming traffic, the source is the external network. This is the address you selected in Step 4 above.

12 Type the destination IP address and port.

   The destination IP address is the internal IP address from your initial setup.

13 Select the **Allow** action.

14 Select the **Enabled** check box.

15 Click **OK** and click **OK** again to create the rule.

Install vCloud Connector Server in vCloud Director 5.1

You can install a vCloud Connector server in vCloud Director 5.1.

You must have at least organization administrator access in the vCloud Director cloud in which you install the vCloud Connector server.

NOTE If you install vCloud Connector server in a public cloud, you can only connect to public clouds in your vCloud Connector UI.

1 Add the vCloud Connector Server to a vCloud Director 5.1 Catalog as a vApp Template on page 23

Before you can deploy a vCloud Connector server in a vCloud Director 5.1 cloud, you must upload the virtual appliance to a catalog as a vApp template. You do not need to upload an additional template if a template is already uploaded to a master catalog that multiple organizations share.

2 Create the vCloud Connector Server from the Template in a vCloud Director 5.1 Cloud on page 24

After the vCloud Connector Server is added to the vCloud Director 5.1 cloud as a template, you can use it to create a running instance on that cloud.

3 Set Up NAT Mapping for vCloud Connector Server in vCloud Director 5.1 on page 25

If you select a NAT-based network connection when you deploy your vCloud Connector server, you need to set up NAT mapping and firewall rules.

Add the vCloud Connector Server to a vCloud Director 5.1 Catalog as a vApp Template

Before you can deploy a vCloud Connector server in a vCloud Director 5.1 cloud, you must upload the virtual appliance to a catalog as a vApp template. You do not need to upload an additional template if a template is already uploaded to a master catalog that multiple organizations share.

Prerequisites

You must have organization administrator or system administrator access in the vCloud Director cloud in which you install the vCloud Connector server. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 18.

Procedure

1 Log in to the vCloud Director Web console using a supported browser.

2 Click **Catalogs**.

If you log in as system administrator, select your organization first, then click the **Catalogs** tab.

3 Select the catalog to which you want to upload the vCloud Connector server, then click the **vApp Templates** tab.

4 Click the **Upload** icon.

5 In the Upload OVF package as a vApp Template dialog box, click **Browse** and select the vCloud Connector server OVF file that you downloaded.

6 Specify a name and, optionally, a description, for the vApp template.

7 Select the virtual datacenter, catalog, and storage profile for the template.

8 Click **Upload**.

The upload process begins. You can monitor the status of the upload in the **Transfer Progress** popup.

NOTE It may take several seconds after the upload itself has finished for the process to be finalized in the cloud.

Create the vCloud Connector Server from the Template in a vCloud Director 5.1 Cloud

After the vCloud Connector Server is added to the vCloud Director 5.1 cloud as a template, you can use it to create a running instance on that cloud.

Prerequisites

You have System Administrator or Organization Administrator access on the vCloud Director cloud on which you install the vCloud Connector Server.

Procedure

1 In the **vApp Templates** tab of the catalog to which you uploaded the vCloud Connector Server, right-click the name of the Server template and select **Add to My Cloud**.

2 Read and accept the EULA, and click **Next**.

3 Give the Server vApp an easily identifiable name, provide a description, and click **Next**.

Default lease information is displayed. You can modify the leases later through the vApp properties settings.

4 Complete the Configure Resources page.

a Select the virtual datacenter in which to store the Server vApp.

b Provide a name for the virtual machine. This name is displayed in the vCloud Connector UI to identify your Server.

c Select a Storage Profile.

d Click **Next.**

5 Select an appropriate network from the **Destination** drop-down menu.

Unless all your vCloud Connector Nodes and the vCloud Connector Server are behind the same firewall, you need to select a network that is configured to access the Internet. Ask your Service Provider or Network Administrator for more information.

6 Select the appropriate IP Assignment from the drop-down menu and click **Next**.

If there is a static IP pool, that is probably a reasonable choice. Ask your Service Provider or Network Administrator for more information. If your provider uses NAT, you will need to set up NAT mapping after your Server is deployed. See "Set Up NAT Mapping for vCloud Connector Server in vCloud Director 5.1," on page 25.

7 In the Networking Properties page, use the information you collected before you began installing vCloud Connector to specify the DNS server, IP address, Netmask, and Default Gateway. If you are using DHCP, leave the fields blank.

8 In the Ready to Complete page, review your settings and click **Finish**.

9 Click the **My Cloud** tab, then select **vApps** in the My Cloud panel.

You can see the vApp being created in the vApps section.

10 Select **VMs** in the My Cloud panel, right-click your vCloud Connector Server, and select **Properties**.

11 In the Virtual Machine Properties page, click the **Guest OS Customization** tab.

12 Check **Enable guest customization**.

13 Click **OK**.

14 In the My Cloud panel, select **vApps**, then right-click the console icon of your vCloud Connector Server and select **Start**.

15 When the vCloud Connector Server is in running state, click **VMs** in the My Cloud panel and make a note of the IP address of your Server.

You need the IP address later in the registration process.

Set Up NAT Mapping for vCloud Connector Server in vCloud Director 5.1

If you select a NAT-based network connection when you deploy your vCloud Connector server, you need to set up NAT mapping and firewall rules.

There are multiple approaches to managing this issue. Decide whether you wish to use NAT to forward only the ports necessary for vCloud Connector operation or to forward all ports and then set up a firewall rule to filter all but the required ports. See "Check System Requirements," on page 16 for the list of required ports.

Prerequisites

Your appliance is deployed and you are logged in to the vCloud Director Web console.

Procedure

1 Click the **Administration** tab and select **Virtual Datacenters** in the left panel.

2 Double-click your virtual datacenter.

3 Click the **Org VDC Networks** tab.

4 Find the network you are using in the list of networks, right-click, and select **Configure Services**.

5 Click the **NAT** tab.

6 Click **Add DNAT** to add the rule.

The Add Destination NAT Rule pop-up appears.

7 Specify the external IP address.

8 If you wish to NAT all ports, enter * for the first port entry.

If you wish to NAT only the required ports, create a rule for each port.

9 Enter the internal IP address from your initial setup and match the port entry for this rule.

10 Click **OK** and click **OK** again.

11 If you are using a firewall rule to control traffic, click the **Firewall** tab and select the **Enable firewall** check box.

12 Click **Add** at the bottom of the page to create a new firewall rule.

Create a rule for each required port.

The Add Firewall Rule popup appears.

13 Select the **Enabled** check-box.

14 Give the rule a name.

15 Type the source IP address and the source port.

For incoming traffic, the source is the external network. This is the address you selected in Step 7 above.

16 Type the destination IP address and port.

The destination IP address is the internal IP address from your initial setup.

17 Select the protocol.

18 Select **Allow**.

19 Click **OK** and click **OK** again to create the rule.

Install vCloud Connector Server in vCloud Director 5.5

You can install a vCloud Connector server in vCloud Director 5.5.

You must have at least organization administrator access in the vCloud Director cloud in which you install the vCloud Connector server.

NOTE If you install vCloud Connector server in a public cloud, you can only connect to public clouds in your vCloud Connector UI.

---

1 Add the vCloud Connector Server to a vCloud Director 5.5 Catalog as a vApp Template on page 26

Before you can deploy a vCloud Connector server in a vCloud Director 5.5 cloud, you must upload the virtual appliance to a catalog as a vApp template. You do not need to upload an additional template if a template is already uploaded to a master catalog that multiple organizations share.

2 Create the vCloud Connector Server from the Template in a vCloud Director 5.5 Cloud on page 27

After the vCloud Connector server is added to the vCloud Director 5.5 cloud as a template, you can use it to create a running instance on that cloud.

3 Set Up NAT Mapping for vCloud Connector Server in vCloud Director 5.5 on page 28

If you select a NAT-based network connection when you deploy your vCloud Connector server, you need to set up NAT mapping and firewall rules.

Add the vCloud Connector Server to a vCloud Director 5.5 Catalog as a vApp Template

Before you can deploy a vCloud Connector server in a vCloud Director 5.5 cloud, you must upload the virtual appliance to a catalog as a vApp template. You do not need to upload an additional template if a template is already uploaded to a master catalog that multiple organizations share.

Prerequisites

You must have organization administrator or system administrator access in the vCloud Director cloud in which you install the vCloud Connector server. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 18.

Procedure

1 Log in to the vCloud Director Web console using a supported browser.

2 Click **Catalogs**.

If you log in as system administrator, click the **Manage & Monitor** tab, select your organization, then click the **Catalogs** tab.

3 Double-click the catalog to which you want to upload the vCloud Connector server.

Verify that the **vApp Templates** tab is displayed.

4 Click the **Upload** icon.

If you are prompted to install the Client Integration Plug-in, follow the link to download and install it, then click the **Upload** icon again.

5 If the Client Integration Access Control dialog box appears, click **Allow**.

6 In the Upload OVF package as a vApp Template dialog box, do the following.

   a Under **Source**, select **Local file**, click **Browse**, and select the vCloud Connector server OVF file that you downloaded.

   b Under **Destination**, type a name and description for the vApp template.

7 Specify a name and, optionally, a description, for the vApp template.

8 Click **Upload**.

The upload process begins. You can monitor the status of the upload in the **Transfer Progress** popup.

NOTE It may take several seconds after the upload itself has finished for the process to be finalized in the cloud.

Create the vCloud Connector Server from the Template in a vCloud Director 5.5 Cloud

After the vCloud Connector server is added to the vCloud Director 5.5 cloud as a template, you can use it to create a running instance on that cloud.

Prerequisites

You have system administrator or organization administrator access on the vCloud Director cloud in which you install the vCloud Connector server.

Procedure

1 In the **vApp Templates** tab of the catalog to which you uploaded the vCloud Connector server, right-click the name of the server template and select **Add to My Cloud**.

2 Read and accept the EULA, and click **Next**.

3 Specify an easily identifiable name for the vApp, and a description.

4 Select a virtual datacenter for the vApp, and click **Next**.

5 Click the **My Cloud** tab, then select **vApps** in the My Cloud panel.

   You can see the vApp being created in the vApps section.

6 Select **VMs** in the My Cloud panel, right-click your vCloud Connector server virtual machine, and select **Properties**.

7 In the Virtual Machine Properties page, click the **Guest OS Customization** tab.

8 Check **Enable guest customization**.

9 Click **OK**.

10 In the My Cloud panel, select **vApps**, then right-click your vCloud Connector server vApp and select **Start**.

11 When the vCloud Connector server is in running state, click **VMs** in the My Cloud panel and make a note of the IP address of your server.

   You need the IP address later in the registration process.

Set Up NAT Mapping for vCloud Connector Server in vCloud Director 5.5

If you select a NAT-based network connection when you deploy your vCloud Connector server, you need to set up NAT mapping and firewall rules.

There are multiple approaches to managing this issue. Decide whether you wish to use NAT to forward only the ports necessary for vCloud Connector operation or to forward all ports and then set up a firewall rule to filter all but the required ports. See "Check System Requirements," on page 16 for the list of required ports.

Prerequisites

Your appliance is deployed and you are logged in to the vCloud Director Web console.

Procedure

1 Click the **Administration** tab and select **Virtual Datacenters** in the left panel.

2 Double-click your virtual datacenter.

3 Click the **Org VDC Networks** tab.

4 Find the network you are using in the list of networks, right-click, and select **Configure Services**.

5 Click the **NAT** tab.

6 Click **Add DNAT** to add the rule.

The Add Destination NAT Rule dialog box appears.

7 Specify the external IP address.

8 If you wish to NAT all ports, select **ANY** for the first port entry.

If you wish to NAT only the required ports, create a rule for each port.

9 Enter the internal IP address from your initial setup and match the port entry for this rule.

10 Click **OK**.

11 If you are using a firewall rule to control traffic, click the **Firewall** tab and select the **Enable firewall** check box.

12 Click **Add** at the bottom of the page to create a new firewall rule.

Create a rule for each required port.

The Add Firewall Rule dialog box appears.

13 Select the **Enabled** check-box, if it is not already selected.

14 Give the rule a name.

15 Type the source IP address and the source port.

For incoming traffic, the source is the external network. This is the address you selected in Step 7 above.

16 Type the destination IP address and port.

The destination IP address is the internal IP address from your initial setup.

17 Select the protocol.

18 Select **Allow**.

19 Click **OK** to create the rule.

Configure vCloud Connector Server

You use the vCloud Connector server Admin Web console to do basic configuration tasks, such as defining your time zone, specifying proxy servers, or setting log levels. What you need to do depends on your particular installation.

NOTE Do not use Firefox to log in to the vCloud Connector server and node Admin Web consoles. Some tabs, such as the Server tab in the server Admin Web console and the Node tab in the node Admin Web console, display blank pages on Firefox.

Prerequisites

The vCloud Connector server is running and you have the IP address for it that you wrote down when you installed it. You also have the information you gathered in "Collect Necessary Information," on page 14.

Procedure

1 Go to the vCloud Connector server Admin Web console at https://*vCC Server IP address*:5480.

2 If you receive a certificate warning, accept the certificate.

3 Log in to the server Admin Web console as **admin**.

The default password is **vmware**.

Check the Web console title to confirm that you are configuring the vCloud Connector server.

4 Use the information you collected in "Collect Necessary Information," on page 14 to complete general configuration.

5 When you have finished with general configuration, keep the server Admin Web console page open at the **Server** tab.

System Tab (Server)

The **System** tab provides general information about the vCloud Connector server virtual appliance, allows you to configure time zones, and lets you shut down or reboot the appliance.

Information

The **Information** tab provides information about the virtual appliance, such as the version number, host name, and OS name. You can also reboot and shut down the server from here.

Time Zone

The **Time Zone** tab allows you to set your local time zone. Select a time zone, then click **Save Settings**.

The virtual hardware clock is always maintained in UTC, which the virtual appliance converts to local time. Correct local time is important for the update repository and VMware Update Manager.

NOTE Changes in time zone settings are not reflected in logs until the service is reset. Click **Reboot** in the **Information** tab to restart the service.

Network Tab (Server)

The **Network** tab lets you view network related information about the appliance, switch between DHCP and static IP addresses, and set up proxy information.

Status

The **Network Status** tab provides already configured network information about your appliance, such as DNS servers, network interfaces, and IP addresses. Click **Refresh** to update your information.

Address

The **Network Address Settings** tab allows you to specify static IP information for your appliance or to retrieve IP settings from a DHCP server.

NOTE If you set a static IP address you must make sure that there are values for all the displayed fields. In vCloud Director installations, you must set Preferred and Alternate DNS servers manually. Talk to your service provider or network administrator for the appropriate addresses. You recorded the information that you need for these settings in "Collect Necessary Information," on page 14.

For more information about network paths in data transfers, see Chapter 9, "Cross-Cloud Data Transfer and Network Connectivity," on page 79.

Click **Save Settings** to accept any changes that you made to the network address settings. Click **Cancel Changes** to discard the changes.

NOTE If you are using static IP settings, and you update the host name and IP settings at the same time, only the IP settings are saved. The host name is not saved. Update the **Hostname** field separately.

Also note that if you change the IP address, you will not see your changes until you log out and log back in to the Admin Web console using the new IP address.

Proxy

The **Proxy Settings** tab allows you to specify any necessary proxy settings, including the HTTP proxy server IP address, port, and, if required, the user name and password. Set these if the vCloud Connector server must use a proxy to reach systems beyond the firewall at the installation location.

NOTE In the **Proxy Username** field, specify a user name that contains lower-case, alpha-numeric characters only and does not exceed 50 characters. Do not use email addresses or domain names (for example, user@company.com or xyz\user) or names that contain a period (for example, firstname.lastname) as special characters are not supported for this field.

Click **Save Settings** to accept any changes that you made to the proxy settings. Click **Cancel Changes** to discard the changes.

Update Tab (Server)

The **Update** tab allows you to check the update status of your virtual appliance and to set your update policy.

Status

The **Status** section allows you to view information about your virtual appliance or to check for and install updates.

Click **Check Updates** to check for updates from the update repository, shown in the **Available Updates** pane. Click **Install Updates** to install the updates.

Settings

The **Update Settings** section allows you to configure automatic updates.

To check for updates automatically	Select **Automatic check for updates**, then set the frequency for the update check.
To check for updates and install the updates automatically	Select **Automatic check and install updates**, then select the frequency for the update check.
To deselect automatic update settings	Select **No automatic updates**.
To update from the default repository	Select **Use Default Repository**. This option is selected by default. Leave this option selected unless you need to update from a specific repository or a CDROM.
To update from a CDROM	Select **Use CDROM Updates**.
To update from a specific repository	Select **Use Specified Repository** and type the user name and password for the repository, if required.

Save any changes you make by clicking **Save Settings**.

Server Tab

The **Server** tab has two parts. One part allows you to change the server administrator password, adjust log levels, and manage SSL certificates. The other part is used later, in the registration process.

General

The **General Settings** section allows you to change the administrator password for the vCloud Connector server, provide a license key to enable advanced features in the vCloud Connector Advanced edition, set log file severity levels, and download log files.

Change admin user password	Specify a new administrator password for the vCloud Connector server, then click **Confirm new password**. You should change the default password.
vCC License	To enable advanced features that are available in the vCloud Connector Advanced edition, enter a valid vCloud Suite 5.1 or 5.5 license key, then click **Update Key**.
Log levels	Set the severity level for vCloud Connector server log files, then click **Change log level**.
Download logs	Click to download a zip file of vCloud Connector server log files.

SSL

The **Manage SSL Certificates** section allows you to disable or enable SSL and to manage your certificates. The vCloud Connector server has SSL disabled by default and includes a self-signed certificate. Before going into production, replace the certificate with a valid certificate.

Disable SSL/Enable SSL	Select **Enable SSL** if you want to enable HTTPS communication. When you enable SSL, the port used to communicate with the vCloud Connector server changes from 80 to 443. If you enable SSL for the server, replace its self-signed certificate with a valid certificate.
Key Information	Displays information about the default key provided.
Certificate Information	Displays information about the self-signed certificate that is provided with the vCloud Connector server.
Generate New Key	If you need to generate a new private key to obtain a valid certificate from your Certificate Authority, specify the required information and click **Generate Key**. In the **Common Name** field, specify the IP address or fully-qualified domain name of the vCloud Connector server. For example, **`10.10.10.10`** or **`myServer.mycompany.com`**. You can only generate a 1024-bit key from the UI; to generate a 2048-bit key, use the command line interface.

Generate and download CSR	Click to create a Certificate Signing Request and save it to your computer. Use the saved hcserver.csr file to get a certificate from your Certificate Authority.
Upload a new X.509 SSL Certificate	When you have your certificate, use the **Browse** button to locate it, then click **Upload**.

For more information on installing valid certificates, see "Add Valid SSL Certificates," on page 71.

vSphere Client Tab

The vSphere Client tab is used to register the vCloud Connector UI. For more information, see "Register the vCloud Connector UI," on page 50.

Nodes Tab (Server)

The **Nodes** tab in the server Admin Web console lets you register vCloud Connector nodes with your vCloud Connector server, download node log files, and register Stretch Deploy settings

Manage Nodes

In the **Manage Nodes** section, you can view the vCloud Connector nodes that are currently registered with the vCloud Connector server, view the status of the nodes, and perform tasks related to nodes.

Table 3-8. Options

Task	
To register a node with the server	Click **Register Node**. See "Register vCloud Connector Nodes with vCloud Connector Server," on page 49.
To edit a node's registration	Click the gears icon next to the node and select **Edit**.
To unregister a node from the server	Click the gears icon next to the node and select **Unregister**.
To download node log files	Click the gears icon next to the node and select **Download Logs**.
To specify Stretch Deploy settings	Click the gears icon next to the node and select **Stretch Deploy Settings**. See Using Stretch Deploy in *Using vCloud Connector*.
To unregister Stretch Deploy settings	Click the gears icon next to the node and select **Unregister Stretch Deploy Settings**. See Using Stretch Deploy in *Using vCloud Connector*.

Install vCloud Connector Nodes

You can install vCloud Connector nodes in vSphere or vCloud Director clouds.

You must install a vCloud Connector node in every cloud you want to connect and oversee using vCloud Connector. To connect public vClouds, you can either install a node in your organization in the public vCloud or use a multi-tenant node installed by the service provider.

vCloud Connector does not require every organization in a vCloud Director cloud to install its own node in the cloud. Public vCloud service providers or administrators of private vCloud Director clouds can install a node in the cloud as a multi-tenant node for multiple customers to use. See Chapter 5, "Deploying Multi-tenant Nodes as a vCloud Service Provider," on page 55 for more information.

To use a multi-tenant node, you need to get the node URL from the service provider or system administrator. See "Use Service Provider Nodes," on page 57 for more information.

Install vCloud Connector Node in vSphere

You can install a vCloud Connector node in vSphere.

For information on installing vCloud Connector in a Linked Mode vCenter server configuration, see "Installing vCloud Connector in Linked Mode vCenter Server Configurations," on page 19.

Prerequisites

You must have administrator-level access in the vSphere cloud in which you install the vCloud Connector node. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 18.

Procedure

1 Log in to vSphere Client.

2 Select **File > Deploy OVF template**.

3 Click **Browse** and navigate to the OVF directory of the node zip file you downloaded to your desktop in "Download the vCloud Connector Virtual Appliances," on page 18.

4 Click **Next**.

5 Proceed through the wizard.

You can either use the Networking Properties step in the wizard to set basic network properties or you can wait and set those properties when you configure your node. Set proxy information during the configuration step.

NOTE If you are going to use a static IP address, you need to assign it here.

6 In vSphere Client, select **Inventory > VMs and Templates** to see the created virtual machine in the hierarchy tree.

7 Right-click the virtual machine and select **Power > Power on** to power on the machine.

8 Click the **Summary** tab and find the vCloud Connector node's IP address in the **General** section. The **IP address** field (not the **Host** field) displays the IP address of the node. Make a note of the IP address. You will need it later in the process.

Install vCloud Connector Node in vCloud Director 1.5

You install a vCloud Connector node in each vCloud Director 1.5 cloud you want to connect and use with vCloud Connector.

If you are a public vCloud service provider or the administrator of a private vCloud Director cloud, you can choose to install a vCloud Connector node in the cloud as a multi-tenant node, instead of having each organization or customer install their own node. A single vCloud Connector node can be used by multiple organizations on the cloud to transfer content to and from the cloud.

If you choose to install a vCloud Connector node as a multi-tenant node, you need to do the following.

- Install a node in the cloud.
- Configure the node.
- Provide information about the node (the node URL) to each organization that will use it.

See Chapter 5, "Deploying Multi-tenant Nodes as a vCloud Service Provider," on page 55 for more information.

If you are a user, that is, an organization, of a public or private vCloud Director cloud, you need to do the following.

- Check with your service provider or system administrator if a vCloud Connector node is already deployed on the cloud as a multi-tenant node.
- If a multi-tenant node is deployed on the cloud, you need to get information about the node (the node URL) from the service provider or system administrator. You require this information to register the node with your vCloud Connector server.
- If a multi-tenant node is not deployed on the cloud, follow the procedures in this section to install a node for your organization.

Procedure

1 Add the vCloud Connector Node to a vCloud Director 1.5 Catalog as a vApp Template on page 34

Before you can deploy a vCloud Connector node in a vCloud Director 1.5 cloud, you must upload the virtual appliance to a catalog as a vApp template. If the template has already been uploaded and put in a master catalog shared by multiple organizations, you can skip this step.

2 Create the vCloud Connector Node from the Template in a vCloud Director 1.5 Cloud on page 35

After the vCloud Connector node is added to the vCloud Director 1.5 cloud as a template, you can use it to create a running instance on that cloud.

3 Set Up NAT Mapping for vCloud Connector Node in vCloud Director 1.5 on page 36

If you select a NAT-based network connection when you deploy your vCloud Connector node, you need to set up NAT mapping and firewall rules.

Add the vCloud Connector Node to a vCloud Director 1.5 Catalog as a vApp Template

Before you can deploy a vCloud Connector node in a vCloud Director 1.5 cloud, you must upload the virtual appliance to a catalog as a vApp template. If the template has already been uploaded and put in a master catalog shared by multiple organizations, you can skip this step.

Prerequisites

You must have system administrator or organization administrator access on the vCloud Director cloud in which you install the vCloud Connector node. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 18.

Procedure

1 Log in to the vCloud Director Web console using a supported browser.

2 Click **Catalogs**.

If you log in as system administrator, select your organization first, then click the **Catalogs** tab.

3 Double-click the catalog to which you want to upload the vCloud Connector node, then click the **vApp Templates** tab.

4 Click the **Upload** icon.

5 In the Upload OVF package as a vApp Template dialog box, click **Browse**, accept the security certificate if you are prompted to do so, and select the node OVF file that you downloaded.

6 Specify a name and, optionally, a description, for the vApp template.

7 Select the virtual datacenter and catalog for the template.

8 Click **Upload**.

The upload process begins. You can monitor the status of the upload in the **Transfer Progress** popup.

NOTE It may take several seconds after the upload itself has finished for the process to be finalized in the cloud.

Create the vCloud Connector Node from the Template in a vCloud Director 1.5 Cloud

After the vCloud Connector node is added to the vCloud Director 1.5 cloud as a template, you can use it to create a running instance on that cloud.

Prerequisites

You have system administrator or organization administrator access in the vCloud Director in which you install the vCloud Connector node.

Procedure

1 In the **vApp Templates** tab of the catalog to which you uploaded, right-click the name of your vCloud Connector node template and select **Add to My Cloud**.

2 Give the node vApp an easily identifiable name and provide a description.

3 Set the leases for the node vApp, then click **Next.**

4 Read and accept the EULA, and click **Next**.

5 Select an appropriate network from the **Network** drop-down menu.

Unless all the nodes controlled by your vCloud Connector server are behind the same firewall, you need to select a network that is configured to access the Internet. Ask your service provider or network administrator for more information.

6 Select the appropriate IP Assignment from the drop-down menu and click **Next**.

If there is a static IP pool, that is probably a reasonable choice. Ask your service provider or network administrator for more information. If your provider uses NAT, you will need to set up NAT mapping after your node is deployed. See "Set Up NAT Mapping for vCloud Connector Node in vCloud Director 1.5," on page 36.

7 In the Networking Properties page, use the information you collected before you began installing vCloud Connector to specify the DNS server, IP address, Netmask, and Default Gateway. If you are using DHCP, leave the fields blank.

8 In the Configure Networking page, leave both check boxes unchecked and click **Next**.

9 In the Ready to Complete page, review the settings and click **Finish**.

10 Click the **My Cloud** tab, then select **vApps** in the My Cloud panel.

You see the vApp being created.

11 In the My Cloud panel, select **VMs**, then right-click your vCloud Connector node virtual machine and select **Properties**.

12 In the Virtual Machine Properties page, click the **Guest OS Customization** tab.

13 Check **Enable guest customization**, then click **OK**.

14 In the My Cloud panel, select **vApps**, then right-click the console icon of the vCloud Connector node and select **Start**.

15 When the vCloud Connector node on vCloud Director 1.5 is in running state, click **VMs** in the My Cloud panel and make a note of the IP address of the vCloud Connector node virtual machine.

You need the IP address later in the registration process.

Set Up NAT Mapping for vCloud Connector Node in vCloud Director 1.5

If you select a NAT-based network connection when you deploy your vCloud Connector node, you need to set up NAT mapping and firewall rules.

There are multiple approaches to managing this issue. Decide whether you wish to use NAT to forward only the ports necessary for vCloud Connector operation or to forward all ports and then set up a firewall rule to filter all but the required ports. See "Check System Requirements," on page 16 for the list of required ports.

Prerequisites

Your appliance is deployed and you are logged in to the vCloud Director Web console.

Procedure

1 Click the **Administration** tab and select **Networks** in the left panel.

2 Find the network you are using in the Networks list, right-click and select **Configure Services**.

3 In the Configure Services dialog box, click the **NAT Mapping** tab and click **Add** at the bottom of the tab to create the NAT rule.

The Add NAT Rule popup appears.

4 Select one of the External IP addresses from the drop-down menu.

Note this address if you plan to set up a firewall rule.

5 If you wish to NAT all ports, enter * for the first port entry.

If you wish to NAT only the required ports, create a rule for each port.

6 Enter the internal IP address from your initial setup and match the port entry for this rule.

7 Click **OK** and click **OK** again.

8 If you are using a firewall rule to control traffic, click the **Firewall** tab and select the **Enable firewall** check box.

9 Click **Add** at the bottom of the pop-up to create a new firewall rule.

Create a rule for each necessary port.

The Add Firewall Rule popup appears.

10 Give the rule a name and select the **Incoming** option.

11 Type the source IP address and the source port.

For incoming traffic, the source is the external network. This is the address you selected in Step 4 above.

12 Type the destination IP address and port.

The destination IP address is the internal IP address from your initial setup.

13 Select the **Allow** option.

14 Select the **Enabled** option.

15 Click **OK** and click **OK** again to create the rule.

Install vCloud Connector Node in vCloud Director 5.1

You install a vCloud Connector node in each vCloud Director 5.1 cloud you want to connect and use with vCloud Connector.

If you are a public vCloud service provider or the administrator of a private vCloud Director cloud, you can choose to install a vCloud Connector node in the cloud as a multi-tenant node, instead of having each organization or customer install their own node. A single vCloud Connector node can be used by multiple organizations on the cloud to transfer content to and from the cloud.

If you choose to install a vCloud Connector node as a multi-tenant node, you need to do the following.

- Install a vCloud Connector node in the cloud.
- Configure the node.
- Provide information about the node (the node URL) to each organization that will use it.

See Chapter 5, "Deploying Multi-tenant Nodes as a vCloud Service Provider," on page 55 for more information.

If you are a user, that is, an organization, of a vCloud Director public or private cloud, you need to do the following.

- Check with your service provider or system administrator if a vCloud Connector node is already deployed on the cloud as a multi-tenant node.
- If a multi-tenant node is deployed on the cloud, you need to get information about the node (the node URL) from the service provider or system administrator. You require this information to register the node with your vCloud Connector server.
- If a multi-tenant node is not deployed on the cloud, follow the procedures in this section to install a node for your organization.

1 Add the vCloud Connector Node to a vCloud Director 5.1 Catalog as a vApp Template on page 37

   Before you can deploy a vCloud Connector node in a vCloud Director 5.1 cloud, you must upload it to a catalog as a vApp template. If the template has already been uploaded and put in a master catalog shared by multiple organizations, you can skip this step.

2 Create the vCloud Connector Node from the Template in a vCloud Director 5.1 Cloud on page 38

   After the vCloud Connector node is added to the vCloud Director 5.1 cloud as a template, you can use it to create a running instance on that cloud.

3 Set Up NAT Mapping for vCloud Connector Node in vCloud Director 5.1 on page 39

   If you select a NAT-based network connection when you deploy your vCloud Connector node, you need to set up NAT mapping and firewall rules.

Add the vCloud Connector Node to a vCloud Director 5.1 Catalog as a vApp Template

Before you can deploy a vCloud Connector node in a vCloud Director 5.1 cloud, you must upload it to a catalog as a vApp template. If the template has already been uploaded and put in a master catalog shared by multiple organizations, you can skip this step.

Prerequisites

You must have system administrator or organization administrator access on the vCloud Director cloud in which you install the vCloud Connector node.

Procedure

1 Log in to the vCloud Director Web console using a supported browser.

2 Click **Catalogs**.

   If you log in as System Administrator, select your organization first, then click the **Catalogs** tab.

3 Select the catalog to which you want to upload the vCloud Connector node, then click the **vApp Templates** tab.

4 Click the **Upload** icon.

5 In the Upload OVF package as a vApp Template popup, click **Browse** and select the node OVF file that you downloaded.

6 Specify a name and, optionally, a description, for the vApp template.

7 Select the virtual datacenter, catalog, and storage profile for the template.

8 Click **Upload**.

The upload process begins. You can monitor the status of the upload in the **Transfer Progress** popup.

NOTE It may take several seconds after the upload itself has finished for the process to be finalized in the cloud.

Create the vCloud Connector Node from the Template in a vCloud Director 5.1 Cloud

After the vCloud Connector node is added to the vCloud Director 5.1 cloud as a template, you can use it to create a running instance on that cloud.

Prerequisites

You have system administrator or organization administrator access on the vCloud Director cloud in which you install the vCloud Connector node.

Procedure

1 In the **vApp Templates** tab of the catalog to which you uploaded the vCloud Connector node, right-click the name of the node template and select **Add to My Cloud**.

2 Read and accept the EULA, and click **Next**.

3 Give the node vApp an easily identifiable name, provide a description, and click **Next**.

   Default lease information is displayed. You can modify the leases later through the vApp properties settings.

4 Complete the Configure Resources page.

   a Select the virtual datacenter in which to store the node vApp.

   b Provide a name for the virtual machine.

   c Select a Storage Profile.

   d Click **Next.**

5 Select an appropriate network from the **Destination** drop-down menu.

   Unless all the vCloud Connector nodes controlled by your vCloud Connector server are behind the same firewall, you need to select a network that is configured to access the Internet. Ask your service provider or network administrator for more information.

6 Select the appropriate IP Allocation from the drop-down menu and click **Next**.

If there is a static IP pool, that is probably a reasonable choice. Ask your service provider or network administrator for more information. If your provider uses NAT, you will need to set up NAT mapping after your node is deployed. See "Set Up NAT Mapping for vCloud Connector Node in vCloud Director 5.1," on page 39.

7 In the Networking Properties page, use the information you collected before you began installing vCloud Connector to specify the DNS server, IP address, Netmask, and Default Gateway. If you are using DHCP, leave the fields blank.

8 In the Ready to Complete page, review the settings and click **Finish**.

9 Click the **My Cloud** tab, then select **vApps** in the My Cloud panel.

You see the vApp being created.

10 After the vApp is created, select **VMs** in the My Cloud panel, right-click your vCloud Connector node, and select **Properties**.

11 In the Virtual Machine Properties page, click the **Guest OS Customization** tab.

12 Check **Enable guest customization**.

13 Click **OK**.

14 In the My Cloud panel, select **vApps**, then right-click the console icon of your node and select **Start**.

15 When the node is in running state, select **VMs** in the My Cloud panel and make a note of the IP address of your node.

You need the IP address later in the registration process.

Set Up NAT Mapping for vCloud Connector Node in vCloud Director 5.1

If you select a NAT-based network connection when you deploy your vCloud Connector node, you need to set up NAT mapping and firewall rules.

There are multiple approaches to managing this issue. Decide whether you wish to use NAT to forward only the ports necessary for vCloud Connector operation or to forward all ports and then set up a firewall rule to filter all but the required ports. See "Check System Requirements," on page 16 for the list of required ports.

Prerequisites

Your appliance is deployed and you are logged in to the vCloud Director Web console.

Procedure

1 Click the **Administration** tab and select **Virtual Datacenters** in the left panel.

2 Double-click your virtual datacenter.

3 Click the **Org VDC Networks** tab.

4 Find the network you are using in the list of networks, right-click, and select **Configure Services** from the popup menu.

5 Click the **NAT** tab.

6 Click **Add DNAT** to add the rule.

The Add Destination NAT Rule form appears.

7 Specify the external IP address.

8 If you wish to NAT all ports, enter * for the first port entry.

If you wish to NAT only the required ports, create a rule for each port.

9 Enter the internal IP address from your initial setup and match the port entry for this rule.

10 Click **OK** and click **OK** again.

11 If you are using a firewall rule to control traffic, click the **Firewall** tab and select the **Enable firewall** check box.

12 Click **Add** at the bottom of the page to create a new firewall rule.

Create a rule for each required port.

The Add Firewall Rule popup appears.

13 Select the **Enabled** check-box.

14 Give the rule a name.

15 Type the source IP address and the source port.

For incoming traffic, the source is the external network. This is the address you selected in Step 7 above.

16 Type the destination IP address and port.

The destination IP address is the internal IP address from your initial setup.

17 Select the protocol.

18 Select **Allow**.

19 Click **OK** and click **OK** again to create the rule.

Install vCloud Connector Node in vCloud Director 5.5

You install a vCloud Connector node in each vCloud Director 5.5 cloud you want to connect and use with vCloud Connector.

If you are a public vCloud service provider or the administrator of a private vCloud Director cloud, you can choose to install a vCloud Connector node in the cloud as a multi-tenant node, instead of having each organization or customer install their own node. A single vCloud Connector node can be used by multiple organizations on the cloud to transfer content to and from the cloud.

If you choose to install a vCloud Connector node as a multi-tenant node, you need to do the following.

- Install a vCloud Connector node in the cloud.
- Configure the node.
- Provide information about the node (the node URL) to each organization that will use it.

See Chapter 5, "Deploying Multi-tenant Nodes as a vCloud Service Provider," on page 55 for more information.

If you are a user, that is, an organization, of a vCloud Director public or private cloud, you need to do the following.

- Check with your service provider or system administrator if a vCloud Connector node is already deployed on the cloud as a multi-tenant node.
- If a multi-tenant node is deployed on the cloud, you need to get information about the node (the node URL) from the service provider or system administrator. You require this information to register the node with your vCloud Connector server.
- If a multi-tenant node is not deployed on the cloud, follow the procedures in this section to install a node for your organization.

1 Add the vCloud Connector Node to a vCloud Director 5.5 Catalog as a vApp Template on page 41

Before you can deploy a vCloud Connector node in a vCloud Director 5.5 cloud, you must upload the virtual appliance to a catalog as a vApp template. You do not need to upload an additional template if a template is already uploaded to a master catalog that multiple organizations share.

2 Create the vCloud Connector Node from the Template in a vCloud Director 5.5 Cloud on page 42

After the vCloud Connector node is added to the vCloud Director 5.5 cloud as a template, you can use it to create a running instance on that cloud.

3 Set Up NAT Mapping for vCloud Connector Node in vCloud Director 5.5 on page 42

If you select a NAT-based network connection when you deploy your vCloud Connector node, you need to set up NAT mapping and firewall rules.

Add the vCloud Connector Node to a vCloud Director 5.5 Catalog as a vApp Template

Before you can deploy a vCloud Connector node in a vCloud Director 5.5 cloud, you must upload the virtual appliance to a catalog as a vApp template. You do not need to upload an additional template if a template is already uploaded to a master catalog that multiple organizations share.

Prerequisites

You must have organization administrator or system administrator access in the vCloud Director cloud in which you install the vCloud Connector node. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 18.

Procedure

1 Log in to the vCloud Director Web console using a supported browser.

2 Click **Catalogs**.

If you log in as system administrator, click the **Manage & Monitor** tab, select your organization, then click the **Catalogs** tab.

3 Double-click the catalog to which you want to upload the vCloud Connector node.

Verify that the **vApp Templates** tab is displayed.

4 Click the **Upload** icon.

If you are prompted to install the Client Integration Plug-in, follow the link to download and install it, then click the **Upload** icon again.

5 If the Client Integration Access Control dialog box appears, click **Allow**.

6 In the Upload OVF package as a vApp Template dialog box, do the following.

a Under **Source**, select **Local file**, click **Browse**, and select the vCloud Connector node OVF file that you downloaded.

b Under **Destination**, type a name and description for the vApp template.

7 Specify a name and, optionally, a description, for the vApp template.

8 Click **Upload**.

The upload process begins. You can monitor the status of the upload in the **Transfer Progress** popup.

NOTE It may take several seconds after the upload itself has finished for the process to be finalized in the cloud.

Create the vCloud Connector Node from the Template in a vCloud Director 5.5 Cloud

After the vCloud Connector node is added to the vCloud Director 5.5 cloud as a template, you can use it to create a running instance on that cloud.

Prerequisites

You have system administrator or organization administrator access on the vCloud Director cloud in which you install the vCloud Connector node.

Procedure

1 In the **vApp Templates** tab of the catalog to which you uploaded the vCloud Connector node, right-click the name of the node template and select **Add to My Cloud**.

2 Read and accept the EULA, and click **Next**.

3 Specify an easily identifiable name for the vApp, and a description.

4 Select a virtual datacenter for the vApp, and click **Next**.

5 Click the **My Cloud** tab, then select **vApps** in the My Cloud panel.

You can see the vApp being created in the vApps section.

6 Select **VMs** in the My Cloud panel, right-click your vCloud Connector node virtual machine, and select **Properties**.

7 In the Virtual Machine Properties page, click the **Guest OS Customization** tab.

8 Check **Enable guest customization**.

9 Click **OK**.

10 In the My Cloud panel, select **vApps**, then right-click your vCloud Connector node vApp and select **Start**.

11 When the vCloud Connector node is in running state, click **VMs** in the My Cloud panel and make a note of the IP address of your node.

You need the IP address later in the registration process.

Set Up NAT Mapping for vCloud Connector Node in vCloud Director 5.5

If you select a NAT-based network connection when you deploy your vCloud Connector node, you need to set up NAT mapping and firewall rules.

There are multiple approaches to managing this issue. Decide whether you wish to use NAT to forward only the ports necessary for vCloud Connector operation or to forward all ports and then set up a firewall rule to filter all but the required ports. See "Check System Requirements," on page 16 for the list of required ports.

Prerequisites

Your appliance is deployed and you are logged in to the vCloud Director Web console.

Procedure

1 Click the **Administration** tab and select **Virtual Datacenters** in the left panel.

2 Double-click your virtual datacenter.

3 Click the **Org VDC Networks** tab.

4 Find the network you are using in the list of networks, right-click, and select **Configure Services**.

5 Click the **NAT** tab.

6 Click **Add DNAT** to add the rule.

The Add Destination NAT Rule dialog box appears.

7 Specify the external IP address.

8 If you wish to NAT all ports, select **ANY** for the first port entry.

If you wish to NAT only the required ports, create a rule for each port.

9 Enter the internal IP address from your initial setup and match the port entry for this rule.

10 Click **OK**.

11 If you are using a firewall rule to control traffic, click the **Firewall** tab and select the **Enable firewall** check box.

12 Click **Add** at the bottom of the page to create a new firewall rule.

Create a rule for each required port.

The Add Firewall Rule dialog box appears.

13 Select the **Enabled** check-box, if it is not already selected.

14 Give the rule a name.

15 Type the source IP address and the source port.

For incoming traffic, the source is the external network. This is the address you selected in Step 7 above.

16 Type the destination IP address and port.

The destination IP address is the internal IP address from your initial setup.

17 Select the protocol.

18 Select **Allow**.

19 Click **OK** to create the rule.

Register vCloud Connector Nodes with Clouds

After you install a vCloud Connector node for a cloud, you need to associate it with the cloud.

In a public or private vCloud Director environment in which a vCloud Connector node is deployed as a multi-tenant node for use by multiple organizations, the service provider or system administrator of the cloud performs this task.

Prerequisites

The vCloud Connector node is powered on and you have its IP address.

Procedure

1 Go to the vCloud Connector node Admin Web console at https://*vCCNodeIPaddress*:5480.

2 Log in as **`admin`**. If you have not changed the password, use **`vmware`**, the default password.

3 Click the **Node** tab, then click the **Cloud** tab.

4 In the **Cloud Type** field, select the type of cloud, either **vSphere** or **vCloud Director**.

5 In the **Cloud URL** field, specify the URL of the cloud. You can specify either the IP address of the cloud or its fully qualified domain name (FQDN).

- **`https://CloudIPaddress`**

  For example: **`https://10.10.100.10`**

- **`https://CloudFQDN`**

  For example: **`https://cloud1.company.com`**

6 Select **Ignore SSL Certificate** if the cloud does not have a valid SSL certificate.

NOTE If the cloud has a valid certificate, deselect this option. Also, import the root certificate of the Certificate Authority that issued the cloud's certificate into the trusted keystore of the vCloud Connector node. See "Add CA Root Certificate to Trusted Keystore," on page 75 for information on importing the certificate.

7 Select **Use Proxy** if there is an HTTP proxy server between the vCloud Connector node and the cloud.

NOTE If you select this option, you must also specify proxy settings in the **Network - Proxy** tab.

8 Click **Update Configuration**.

The vCloud Connector node is registered with the cloud.

What to do next

Configure your vCloud Connector node by using the settings in the other tabs of the vCloud Connector node Admin Web console.

Configure vCloud Connector Nodes

You use the vCloud Connector node Admin Web console for each of your nodes to perform basic configuration tasks, such as defining your time zone, specifying proxy servers, or setting log levels. What you need to do depends on your particular installation.

For vCloud Connector nodes deployed as multi-tenant nodes in a public cloud or in a private vCloud Director cloud, the service provider or cloud administrator configures the node.

NOTE Do not use Firefox to log in to the vCloud Connector server and node Admin Web consoles. Some tabs, such as the Server tab in the server Admin Web console and the Node tab in the node Admin Web console, display blank pages on Firefox.

Prerequisites

The vCloud Connector node instance is running and you have the IP address for it that you wrote down when you installed it. You have the information you collected in "Collect Necessary Information," on page 14.

Procedure

1 Go to the vCloud Connector node Admin Web console at https://*NodeIPaddress*:5480.

2 If you receive a certificate warning, accept the certificate.

3 Log in as **`admin`**.

The default password is **`vmware`**.

Check the Web console title to make sure you are configuring the vCloud Connector node.

4 Use the information you collected to complete general configuration as needed.

5 When you finish the general configuration tasks, log out of the vCloud Connector node Admin Web console.

System Tab (Node)

The **System** tab provides general information about the virtual appliance, allows you to set time zones, and lets you shut down or reboot the appliance.

Information

The **Information** tab provides information about the virtual appliance, such as the version number, host name, and OS name. You can also reboot or shut down the virtual appliance from here.

Time Zone

The **Time Zone** tab allows you to set your local time zone. Select a time zone, then click **Save Settings**.

The virtual hardware clock is always maintained in UTC, which the virtual appliance converts to local time. Correct local time is important for the update repository and VMware Update Manager.

NOTE Changes in time zone settings are not reflected in logs until the service is reset. Click **Reboot** in the **Information** tab to restart the service.

Network Tab (Node)

The **Network** tab allows you to view network related information about the appliance, switch between DHCP and static IP addresses, and set up proxy information.

Status

The **Network Status** tab provides already configured network information about your appliance, such as DNS servers, network interfaces, and IP addresses. Click **Refresh** to update your information.

Address

The **Network Address Settings** tab allows you to specify static IP information for your appliance or to retrieve IP settings from a DHCP server.

NOTE If you set a static IP address you must make sure that there are values for all the displayed fields. In vCloud Director installations, you must set Preferred and Alternate DNS servers manually. Talk to your service provider or network administrator for the appropriate addresses. You recorded the information that you need for these settings in "Collect Necessary Information," on page 14.

For more information about network paths in data transfers, see Chapter 9, "Cross-Cloud Data Transfer and Network Connectivity," on page 79.

Click **Save Settings** to accept any changes that you made to the network address settings. Click **Cancel Changes** to discard the changes.

NOTE If you are using static IP settings, and you update the host name and IP settings at the same time, only the IP settings are saved. The host name is not saved. Update the **Hostname** field separately.

Also note that if you change the IP address, you will not see your changes until you log out and log back in to the Admin Web console using the new IP address.

Proxy

The **Proxy Settings** tab allows you to set up any necessary proxy settings, including the HTTP proxy server IP address, port, and a user name and password if the proxy server requires authentication. Set these if the vCloud Connector node must use a proxy to reach systems beyond the firewall at the installation location.

NOTE In the **Proxy Username** field, specify a user name that contains lower-case, alpha-numeric characters only and does not exceed 50 characters. Do not use email addresses or domain names (for example, user@company.com or xyz\user) or names that contain a period (for example, firstname.lastname) as special characters are not supported for this field.

Click **Save Settings** to accept any changes that you made to the proxy settings. Click **Cancel Changes** to discard the changes.

NOTE To set a proxy server for UDT-based copy, set it in the UDT Proxy section in the **Node - General** tab.

Update Tab (Node)

The **Update** tab allows you to check the update status of your virtual appliance and to set your update policy.

Status

The **Status** section allows you to view information about your virtual appliance and to check for and install updates.

Click **Check Updates** to check for updates from the update repository, shown in the **Available Updates** pane. Click **Install Updates** to install the updates.

Settings

The **Update Settings** section allows you to configure automatic updates.

To check for updates automatically	Select **Automatic check for updates**, then set the frequency for the update check.
To check for updates and install the updates automatically	Select **Automatic check and install updates**, then select the frequency for the update check.
To deselect automatic update settings	Select **No automatic updates**.
To update from the default repository	Select **Use Default Repository**. This option is selected by default. Leave this option selected unless you need to update from a specific repository or a CDROM.
To update from a CDROM	Select **Use CDROM Updates**.
To update from a specific repository	Select **Use Specified Repository** and type the user name and password for the repository, if required.

Save any changes you make by clicking **Save Settings**.

Node Tab

The **Node** tab allows you to change the vCloud Connector node administrator password, adjust log levels, and manage SSL certificates. It also lets you select a data transfer protocol and change the maximum number of concurrent tasks. You also use this tab to register the vCloud Connector node with a cloud.

Cloud

In the **Cloud Registration** section, you register the vCloud Connector node with a cloud.

NOTE For public or private vCloud Director clouds that have a vCloud Connector node deployed as a multi-tenant node for use by multiple organizations, this task is performed by the service provider or network administrator of the cloud.

Cloud Type	The type of cloud.
Cloud URL	The URL of the cloud. You can specify either the IP address of the cloud or its fully qualified domain name (FQDN): ■ **`https://CloudIPaddress`** For example: **`https://10.10.100.10`** ■ **`https://CloudFQDN`** For example: **`https://cloud1.company.com`**
Ignore SSL Cert	Select this option if the cloud does not have a valid SSL certificate. NOTE If the cloud has a valid certificate, deselect this option. Also, import the root certificate of the Certificate Authority that issued the cloud's certificate into the trusted keystore of the vCloud Connector node. See "Add CA Root Certificate to Trusted Keystore," on page 75 for information on importing the certificate.
Use Proxy	Select this option if there is an HTTP proxy server between the vCloud Connector node and the cloud. If you select this option, you must also specify proxy settings in the **Network - Proxy** tab.

General

The **General Settings** section allows you to change the administrator password for the vCloud Connector node, set log file severity levels, download log files, select the maximum number of concurrent tasks, and select the data transfer protocol.

Change admin user password	Specify a new administrator password for the vCloud Connector node, then click **Confirm new password**. You should change the default password.
Log levels	Set the severity level for vCloud Connector node log files, then click **Change log level**.
Download logs	Click to download a zip file of vCloud Connector node log files. NOTE If you are using a multi-tenant node that has been deployed by a public vCloud service provider or private vCloud Director cloud system administrator for use by multiple organizations, you do not have access to the node. You can download your log files from the vCloud Connector server Admin Web console.
Concurrent Tasks	Specify the maximum number of concurrent tasks that are allowed for the vCloud Connector node, then click **Change Maximum Concurrent Tasks**. The default is 10. Note that if you increase the maximum number of concurrent tasks, you should also increase the vCloud Connector node storage. The amount of storage you need depends upon the size of your tasks. Approximately 50GB is recommended for each added task. See "Increase Maximum Concurrent Tasks," on page 77 and "Configure vCloud Connector Node Allocated Storage," on page 76 for more information.

UDT	UDT is a data transfer protocol that can be used instead of HTTP(S) to copy data. **UDT Status** displays whether UDT is currently enabled or disabled. Select **Enable UDT** or **Disable UDT** to enable or disable UDT. When UDT is disabled, HTTP(S) is used to copy data. See Chapter 7, "Selecting Copy Options," on page 61 for more information.
UDT Proxy	Specify information about the proxy sever that you want to use with UDT data transfer, then click **Configure UDT Proxy**.

Proxy Server IP address	The IP address of the proxy server. For example, **`10.10.10.10`**.
Port	The SOCKS port.
Username	(Optional) The user name for the proxy server, if the proxy server requires authentication.
Password	(Optional) The password for the proxy server, if the proxy server requires authentication.

NOTE UDT data transfer is only compatible with SOCKS5-compliant proxy servers, as these proxy servers support the UDP protocol. You cannot use UDT data transfer with any other types of proxy servers.

See "Using a Proxy Server with UDT," on page 66 for more information.

Encryption	By default, data is transferred as plain text when UDT is enabled. To enable data encryption with UDT, select **Enable Encryption**. **Encryption Status** displays whether encryption for UDT is currently enabled or disabled in the node. Note that the encryption status on the destination node determines whether UDT transfer is encrypted or decrypted. See "Data Encryption," on page 64 for more information.

SSL

The **Manage SSL Certificates** section allows you to disable or enable SSL and to manage your certificates. vCloud Connector nodes have SSL enabled by default and include a self-signed certificate. Before going into production, replace the certificate with a valid certificate.

Disable SSL/Enable SSL	Select **Disable SSL** if you want to disable HTTPS communication and use HTTP. When you disable SSL, the port that is used to communicate with the node changes from 443 to 80. **NOTE** After you enable or disable SSL for a node, you must update the node's registration with the vCloud Connector server. Note that for copy, the SSL status on the destination node determines whether data transfer to that node is encrypted or unencrypted.
Key Info	Displays information about the default key provided.
Certificate Info	Displays information about the self-signed certificate that is provided with the vCloud Connector node.
Generate New Key	If you need to generate a new private key to obtain a valid certificate from your Certificate Authority, type the required information and click **Generate Key**. In the **Common Name** field, specify the IP address or fully-qualified domain name of the vCloud Connector server. For example, **`10.10.10.10`** or **`myNode.mycompany.com`**. You can only generate a 1024-bit key from the UI; to generate a 2048-bit key, use the command line interface.
Generate and download CSR	Click to create a Certificate Signing Request and save it to your computer. Use the saved hcagent.csr file to get a certificate from your Certificate Authority.
Upload a new X.509 SSL Certificate	Once you have your certificates, use the **Browse** button to locate the root, intermediate, and signed certificates, then click **Upload**. You must upload all three certificates. If your Certificate Authority issues only two certificates, upload them from the command line. See "Upload Certificates from the Command Line," on page 74.

For more information on installing valid certificates, see "Add Valid SSL Certificates," on page 71.

Register vCloud Connector Nodes with vCloud Connector Server

You use the vCloud Connector server Admin Web console to register vCloud Connector nodes with the vCloud Connector server. The nodes can be installed on vSphere, private vCloud Director clouds, or public vClouds. The registration allows the server to manage the nodes.

When you register a node, you can specify the node URL with either the node IP address or fully qualified domain name (FQDN). You must use an FQDN with a proper entry in the DNS server so that the FQDN gets resolved to the correct address.

Prerequisites

To register a multi-tenant node deployed on a public cloud or private vCloud Director cloud, get the node URL from the service provider or cloud administrator.

Procedure

1 Go to the vCloud Connector server Admin Web console at https://*vCCServerIPaddress*:5480.

If you receive a certificate error, accept the certificate. The vCloud Connector server has a self-signed certificate.

2 Log in to the Web console as **admin**.

The default password is **vmware**.

3 Click the **Nodes** tab.

The Manage Nodes tab contains the list of vCloud Connector nodes that are currently registered.

The Local Content Directory node always appears by default. This node is for Content Sync. Do not edit this node.

4 Click **Register Node**.

5 Complete the node information.

Node Info Option	Description
Name	A name for the cloud. The cloud will appear by this name in the vCloud Connector UI.
Description	A description of the node. For example, you can specify whether the node is a service provider node or a local node, or provide information about whom to contact if there are any issues.
URL	The URL of the node. You can specify either the IP address of the node or its FQDN. ■ **https://*vCCNodeIPaddress*** For example: **https://10.10.100.10** ■ **https://*FQDN*** For example: **https://node1.company.com** You can get the URL of the node from its console in the vSphere or vCloud Director cloud in which it is installed. If the node is on a public vCloud, obtain this information from your service provider.
Public	Select if the cloud is a public cloud outside the firewall where your vCloud Connector server is installed.

Node Info Option	Description
Use Proxy	Select if your vCloud Connector server needs to use a proxy to reach the node that you are registering.
Ignore SSL Certificate	Select if you did not install a valid certificate on the node and if SSL is enabled on the node. SSL is enabled on nodes by default. NOTE If you did not install valid certificates, and you do not select this option, copying fails. If you select this option, and later install a valid certificate, you must deselect this option and restart the vCloud Connector server. NOTE If you are registering a service provider node, obtain this information from your service provider.

6 Complete the cloud information.

Cloud Info Option	Description
Cloud Type	Type of cloud with which the node is associated, either **vSphere** or **vCloud Director**.
vCD Org Name	(For vCloud Director clouds only) Type the name of your organization in the vCloud Director cloud. You must use a valid organization name. vCloud Connector validates the name that you provide with the cloud. Ensure that you use the correct case for the name. If you selected **vSphere** in the **Cloud Type** option, this field is disabled. NOTE If you are registering a service provider node, specify the name of your organization on the public cloud.
Username	User name for the cloud.
Password	Password for the cloud.

7 Click **Register**.

The Register Node with Server window closes and the vCloud Connector node appears in the **Manage Nodes** list. To edit values, unregister the node, or to download log files for a node, click the gears icon at the right of the list entry.

NOTE Do not update or unregister a vCloud Connector node while a task is in progress.

Register the vCloud Connector UI

To use the vCloud Connector UI, you register it to a vSphere Client.

Register the vCloud Connector UI in vSphere Client

Set up the vCloud Connector UI as a plug-in in vSphere Client using the vCloud Connector server Admin Web console.

Register the vCloud Connector UI using a vCenter Server administrator role or any user role that includes Extension privileges.

You can register your vCloud Connector UI with only one vSphere Client at a time. To register with another vSphere Client, unregister and then register with the new vSphere Client.

A vSphere Client can have only one vCloud Connector instance as a plug-in. To replace it, select the **Overwrite existing registration** option while registering.

NOTE Because the vSphere Client interface uses the Internet Explorer rendering engine, it also uses the Internet Explorer security and privacy settings. Set your settings at Medium High or below. This setting allows cookies and Javascript, both of which are necessary for the plug-in to work.

Prerequisites

You need the information you collected in "Collect Necessary Information," on page 14. You need the IP address of the vCloud Connector server and the IP address or fully qualified domain name of the vCenter Server to which the vSphere Client is pointed. You also need an administrator username and password, or any user role that includes Extension privileges, for that vCenter Server.

Procedure

1 Go to the vCloud Connector server Admin Web Console at https://*vCCserverIPaddress*:5480.

2 If you get a certificate error, accept the certificate.

3 Log in as **admin**.

If you have not changed the password, use **vmware**, the default password.

4 Click the **Server** tab, and click the **vSphere Client** tab.

5 Type the vCloud Connector server URL using the format https://*vCCServerIPaddress*.

If you are using DHCP, the **vCC Server URL** text box is automatically populated.

6 Type the vCenter Server IP address or fully qualified domain name.

NOTE If your vCenter Server is running on a port other than the default, make sure you indicate the port along with the IP address.

---

7 Type the user name and password for the vCenter Server.

8 If you have a previously registered version of the vCloud Connector server that you are replacing with this current version, select **Overwrite existing registration**.

9 Click **Register**.

To unregister a previous registration, click **Unregister**. To update an existing registration, click **Update Registration**.

When the registration is completed, a confirmation message appears at the top of the section.

Entering the License Key for vCloud Connector Advanced Edition

4

To enable advanced features available in vCloud Connector Advanced edition (Content Sync and Datacenter Extension, also referred to as Stretch Deploy), you need to enter a valid vCloud Suite 5.1 or 5.5 license key.

Prerequisites

You have installed vCloud Connector. You have a valid vCloud Suite license key.

Procedure

1 Go to the vCloud Connector Server Admin Web console at https://*vCCServerIPaddress*:5480.

   You can get the IP address of the vCloud Connector server from its console in the vSphere or vCloud Director cloud in which you installed it.

2 Log in as **`admin`**. If you have not changed the password, use **`vmware`**, the default password.

3 Click the **Server** tab, then click the **General** tab.

4 In the **vCC License** section, type the license key.

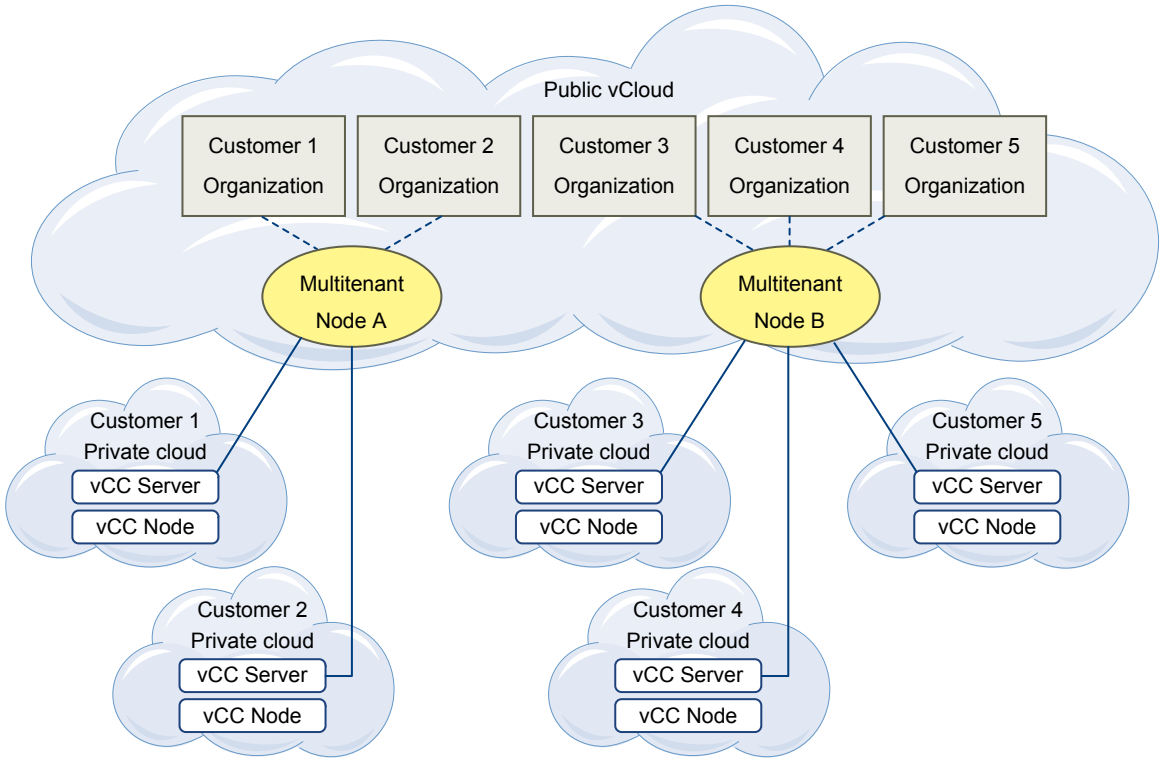
5 Click **Update Key**.

Advanced features in vCloud Connector are now enabled. You can access them in the vCloud Connector UI.

Deploying Multi-tenant Nodes as a vCloud Service Provider

5

Figure 5-1. Multi-tenant Node



vCloud Connector nodes are multi-tenant, that is, one node can be used by multiple tenants to transfer content to and from a cloud.

As a public vCloud service provider (or the administrator of a private vCloud Director cloud serving many departments), you can deploy a multi-tenant node in the cloud for your customers to use, instead of requiring each customer to install a node in their own organization in the cloud.

Each node can support 20 tenants. Depending on the number of tenants, you might need to deploy multiple vCloud Connector nodes.

For example, you might deploy the following nodes.

- Multi-tenant Node A for customers 1-20 on public vCloud 1
- Multi-tenant Node B for customers 21-40 on public vCloud 1

- Multi-tenant Node C for customers 41-60 on public vCloud 2
- Multi-tenant Node D for customers 61-80 on public vCloud 2

After you deploy the nodes, you provide the appropriate node URL to each set of customers for them to register the node with their own vCloud Connector servers.

Deployment Considerations

- As each multi-tenant node is dedicated to a group of customers, vCloud Connector does not support using a load balancer in front of a multi-tenant node.
- Each multi-tenant node can support up to 20 organizations.

Deploying Multi-tenant Nodes

1. Determine how many multi-tenant nodes you need based on the number of customers you intend to support.

   Each node can support 20 organizations.

2. Install vCloud Connector nodes in the public vCloud, one for each set of customers.

   See Chapter 3, "Installing vCloud Connector," on page 13 for more information.

   NOTE You do not need to install a vCloud Connector server.

3. Email the appropriate node URL to each set of customers. Specify either the IP address of the node or its fully qualified domain name (FQDN).

   - **`https://`*`vCCNodeIPaddress`***

     For example: **`https://10.10.100.10`**

   - **`https://`*`vCCNodeFQDN`***

     For example: **`https://node1.company.com`**

4. Ask the customers to register the node with their vCloud Connector servers using the node URL you provided and their own organization credentials.

   See "Register vCloud Connector Nodes with vCloud Connector Server," on page 49.

Each customer will register the multi-tenant node with their own vCloud Connector server, using the URL you provided and their own organization credentials. This enables them to transfer content to and from their organization in the public vCloud.

NOTE If you want to select the **Enable UDT** option in the multi-tenant node to enable UDT-based copy, you can do so only after the node is registered with a customer's vCloud Connector server. UDT cannot be enabled on a node until the node is registered with a server.

Accessing Multi-tenant Node Log Files

As the multi-tenant node administrator, you can access node log files for all customers from the node console or Admin Web console. Log files are divided by organization. See "Accessing Log Files from the Console," on page 89 and "Accessing Log Files from the UI," on page 88 for more information.

Customers do not have access to the multi-tenant node console or Admin Web console. They can access node log files from their vCloud Connector server Admin Web console. See "Accessing Log Files for Multi-tenant Nodes," on page 60 for more information.

Using Service Provider Multi-tenant Nodes

6

To add a public cloud to your vCloud Connector installation, you can use the multi-tenant vCloud Connector node deployed by the service provider in the cloud. You register the multi-tenant node with your own vCloud Connector server, which enables you to add the cloud to the vCloud Connector UI. You can then manage your data on the public cloud and transfer content to and from the public cloud.

This chapter includes the following topics:

Use Service Provider Nodes

You can connect a public vCloud to your vCloud Connector installation by either installing your own vCloud Connector node in your organization in the public cloud or by using a service provider multi-tenant node. To use a service provider node, ask your service provider to install a multi-tenant node in the public cloud and send you the node URL. You can then register the node with your own vCloud Connector server to connect the cloud.

You use the credentials for your organization in the public vCloud and the node URL provided by the service provider to register the node.

NOTE To connect a vCloud Hybrid Service cloud to your vCloud Connector installation, see "Use vCloud Hybrid Service Multi-tenant Nodes," on page 57.

Prerequisites

The service provider has installed a vCloud Connector node in the public cloud as a multi-tenant node.

Procedure

1 Obtain the URL of the multi-tenant node deployed on the public cloud from your service provider.

2 Register the multi-tenant node with your vCloud Connector server using the URL provided by the service provider and your own public vCloud organization credentials.

See "Register vCloud Connector Nodes with vCloud Connector Server," on page 49 for information.

Use vCloud Hybrid Service Multi-tenant Nodes

You can connect a vCloud Hybrid Service cloud to your vCloud Connector installation by using a multi-tenant vCloud Connector node deployed in the vCloud Hybrid Service.

- "Add a Catalog in the vCloud Hybrid Service," on page 59

Register the vCloud Hybrid Service Multi-tenant Node

To connect a vCloud Hybrid Service cloud to your vCloud Connector installation, ask your service provider to install a multi-tenant vCloud Connector node in the vCloud Hybrid Service and send you the node URL. You can then register the multi-tenant node with your vCloud Connector server.

A vCloud Hybrid Service cloud does not appear in vCloud Connector as a single cloud. Each virtual datacenter in the vCloud Hybrid Service cloud appears as a separate cloud in vCloud Connector.

If you have a vCloud Hybrid Service Dedicated Cloud instance, you need to register all the virtual datacenters in the cloud to your vCloud Connector server individually. Similarly, if you have one or more Virtual Private Cloud instances, you need to register each of them them individually with your vCloud Connector server. You do this by registering the multi-tenant node deployed on the cloud with your vCloud Connector server multiple times, once for each virtual datacenter or Virtual Private Cloud instance.

You use your vCloud Hybrid Service credentials and the node URL sent by the service provider to register the node.

Prerequisites

A multi-tenant vCloud Connector node has been installed in the vCloud Hybrid Service.

Procedure

1 Obtain the URL of the multi-tenant vCloud Connector node installed in the vCloud Hybrid Service from your service provider.

2 Go to the vCloud Connector server Admin Web console at https://*vCCServerIPaddress*:5480.

3 Log in as **`admin`**.

The default password is **`vmware`**.

4 Click the **Nodes** tab.

The **Manage Nodes** tab displays the list of nodes that are currently registered with the server. The Local Content Directory node, used for Content Sync, always appears by default.

5 Click **Register Node**.

6 Specify the node information.

Node Info Option	Description
Name	A name for the cloud. The cloud will appear by this name in the vCloud Connector UI.
Description	A description of the vCloud Connector node.
URL	The URL of the node, obtained from your vCloud Hybrid Service provider. The URL will have either the IP address of the node or its fully qualified domain name (FQDN). You must specify port 8443 as part of the URL. ■ **`https://vCCNodeIPaddress:8443`** For example: **`https://10.10.100.10:8443`** ■ **`https://vCCNodeFQDN:8443`** For example: **`https://node1.company.com:8443`**
Public	Select this option.

Node Info Option	Description
Use Proxy	Select this option if your vCloud Connector server needs to go through a proxy server to reach the multi-tenant node on the vCloud Hybrid Service cloud. If you are using a proxy server, you must also specify proxy settings in the **Network - Proxy** tab.
Ignore SSL Certificate	Multi-tenant nodes in vCloud Hybrid Service have SSL enabled and certificates from DigiCert installed. To use the certificate, you must add a DigiCert High Assurance CA-3 intermediate certificate to your vCloud Connector server trusted keystore. See "Add CA Root Certificate to Trusted Keystore," on page 75 for information. If you have added the intermediate certificate to your vCloud Connector server trusted keystore, you can deselect this option. If you have not added the certificate, select this option.

7 Specify the cloud information.

Cloud Info Option	Description
Cloud Type	Select **vCloud Director**.
VCD Org Name	Specify the name of your vCloud Hybrid Service virtual datacenter. You must use a valid name. vCloud Connector validates the name that you provide with the cloud. This field is case-sensitive. Ensure that you use the correct case for the name.
Username	Your vCloud Hybrid Service virtual datacenter user name.
Password	Your vCloud Hybrid Service virtual datacenter password.

8 Click **Register**.

The Register Node with Server window closes and the node appears in the **Manage Nodes** list.

9 Repeat Steps 5 to 8 for each virtual datacenter or Virtual Private Cloud instance that you want to add to vCloud Connector.

Add a Catalog in the vCloud Hybrid Service

To copy virtual machines, vApps, or templates to the vCloud Hybrid Service, you must first add a catalog in the vCloud Hybrid Service. vCloud Hybrid Service clouds do not have user catalogs by default.

You must add a catalog to each virtual datacenter that you connect to your vCloud Connector installation and to which you want to copy data.

Prerequisites

You have virtual infrastructure administrator user privileges in the vCloud Hybrid Service.

Procedure

1 Log in to the vCloud Hybrid Service portal with virtual infrastructure administrator user credentials.

2 Click the virtual datacenter to which you want to add a catalog.

3 Click **Manage Catalogs in vCloud Director**.

4 Cick the **Add** icon to add a catalog.

5 Type a name for the catalog and click **Next**.

6 Click **Add Members** to add users to the catalog.

7 Select **Everyone in the organization**.

8 In the **Access level** drop-down list, select **Read/Write**, and click **OK**.

9 Click **Next**, and click **Finish**.

Accessing Log Files for Multi-tenant Nodes

If you are using a vCloud Connector node that has been deployed as a multi-tenant node by a public vCloud service provider or private vCloud Director system administrator, you do not have access to the vCloud Connector node console or Admin Web console. You can download node log files for your own organization from your vCloud Connector server Admin Web console.

Procedure

1 Go to your vCloud Connector server Admin Web console at https://*vCCServerIPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Click the **Nodes** tab.

4 Click the gears icon next to the multi-tenant node that you registered with your server, and select **Download Logs**.

5 Save the zip file.

6 Extract files from the zip file.

The node log file is named hca.log and is in the `opt/vmware/hcagent/logs` directory.

7 Selecting Copy Options

Copy options are configured in the vCloud Connector nodes associated with the source and destination clouds. You can select the data transfer protocol used for copy. You can also choose to use data encryption with copy.

Copy settings apply to all copy operations, when you use the Copy command directly or when data is copied as part of features such as Content Sync or Datacenter Extension.

This chapter includes the following topics:

About vCloud Connector Copy

vCloud Connector 2.5 features a new path-optimized copy mechanism that provides a higher copy speed and lower storage requirements.

It uses a path optimization framework to export data from the source cloud, transfer it, and import it into the destination cloud in a parallel flow, instead of sequentially.

The data is streamed in small chunks. As data is being exported from the source cloud, it is transferred and imported into the destination cloud.

Unlike in previous versions of vCloud Connector, files are not written to the staging area of either the source or destination vCloud Connector node during the copy process.

Under optimal conditions, the node staging area is not used during copy. However, in some scenarios (for example, if the transfer or import part of the copy process is slower than the export), data needs to be buffered and the staging area is used to store chunks of data. In such cases, the amount of storage needed might be equivalent to the size of the object being copied. Ensure that you have adequate storage on the nodes. See "Configure vCloud Connector Node Allocated Storage," on page 76 for information on adding storage.

NOTE Checkpoint restart is not supported if the node associated with the source or destination cloud is restarted while a copy task is in progress. You need to copy the object again.

Compatibility with Earlier Versions of vCloud Connector

The new, path-optimized copy mechanism is compatible with earlier versions of vCloud Connector.

The following table lists which copy mechanism is used when the vCloud Connector nodes in the source and destination clouds are of different versions.

Table 7-1. Compatibility with Earlier Versions

Node A Version	Node B Version	Copy Mechanism Used
2.5	2.5	New path-optimized copy
2.5	2.0	Old, 2.0 copy mechanism
2.0	2.5	Old, 2.0 copy mechanism
2.0	2.0	Old, 2.0 copy mechanism

In new installation or upgrade scenarios, your vCloud Connector nodes in the source and destination clouds will be of the same version.

In scenarios where a vCloud Connector node is deployed as a multi-tenant node, you might have different versions of the node on the source and destination clouds. For example, if you are using a service provider node on a public vCloud, the service provider node might be of a different version than the node in your private cloud.

NOTE As the UDT copy protocol is only available in vCloud Connector version 2.5, it can be used only if both the source and destination nodes are version 2.5. If one of the nodes is an older version, the default HTTP(s) copy protocol is used regardless of whether UDT is selected.

Data Transfer Protocols for Copy

You can select the data transfer protocol you want to use for copying data with vCloud Connector. The protocol is used when you copy data with the Copy command as well as when data is copied for features such as Content Sync and Datacenter Extension.

vCloud Connector supports two data transfer protocols.

- HTTP(S)

  The HTTP(S) protocol is the default protocol in vCloud Connector.

  By default, data is encrypted with this protocol, that is, HTTPS is used. You can choose to deselect encryption. See "Data Encryption," on page 64.

  With HTTP(S), data transfer occurs over port 443 when SSL is enabled and over port 80 when SSL is disabled.

- UDT

  UDT is a reliable, high-speed data transfer protocol based on UDP (User Datagram Protocol). UDT offers significantly higher speeds for transfer over high-latency, high-bandwidth networks.

  By default, data is transferred as plain text with the UDT protocol. You can choose to encrypt data. See "Data Encryption," on page 64.

  With UDT, data transfer occurs over a dynamically-generated port on the source node and port 8190 on the destination node. Any firewall rules must allow for this type of connection for UDT-based data transfer. (When you copy data between a private cloud and a public cloud, data transfer is between a dynamically-generated port on the private cloud node and port 8190 on the public cloud node. Port 8190 must be open in the public cloud.)

If you use a proxy server with UDT, communication between the local node and the proxy server occurs with two separate connections. See "Using a Proxy Server with UDT," on page 66 for more information.

By default, vCloud Connector uses HTTP(s) as the data transfer protocol. To use UDT, you need to select the **Enable UDT** option in the vCloud Connector Node Admin Web console for both the source and destination nodes. Note that if UDT is enabled in only one of the nodes, the default protocol, HTTP(s), will be used.

View Which Data Transfer Protocol is Currently Selected

You can view which data transfer protocol is currently selected by looking at the UDT Status setting in the node Admin Web console. HTTP(S) is the default protocol and is used unless UDT has been selected in the node Admin Web console for both the source and destination nodes.

Procedure

1 Go to the vCloud Connector node Admin Web console at https://*vCCNodeIPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Click the **Node** tab, then click the **General** tab.

4 In the **UDT** section, view the **UDT Status**.

If UDT is enabled, UDT is being used as the data transfer protocol. If UDT is disabled, HTTP(S) is being used.

NOTE UDT is used as the data transfer protocol only if it is enabled on both the source and destination nodes. If UDT is enabled in only one of the nodes, the default protocol, HTTP(s), is used.

5 Log out of the node Admin Web console.

Select UDT Protocol for Data Transfer

By default, vCloud Connector uses HTTP(S) for data transfer. To use the UDT data transfer protocol, select the **Enable UDT** option in the vCloud Connector node.

You must select the **Enable UDT** option in both the source and destination vCloud Connector nodes. If you select it in only one of the nodes, the default protocol, HTTP(S), is used for data transfer between the nodes.

NOTE You can enable UDT for a node only after you register the node with your vCloud Connector server.

Procedure

1 Go to the vCloud Connector node Admin Web console at https://*vCCNodeIPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Click the **Node** tab, then the **General** tab.

4 In the **UDT** section, click **Enable UDT**.

The **UDT Status** field displays **Enabled**.

5 If you want to enable data encryption for UDT transfer, in the **Encryption** section, click **Enable Encryption**.

See also "Data Encryption," on page 64 and "Enabling Data Encryption for UDT Data Transfer Protocol," on page 65.

6 Log out of the node Admin Web console.

Select HTTP(S) Protocol for Data Transfer

By default, vCloud Connector uses the HTTP(S) protocol for data transfer. If you enabled UDT, disable it to use HTTP(S).

You should enable HTTP(S) on both the source and destination nodes. However, HTTP(S) will be used as the data transfer protocol even if UDT is enabled on one of the nodes.

Procedure

1 Go to the vCloud Connector node Admin Web console at https://*vCCNodeIPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Click the **Node** tab, then the **General** tab.

4 In the **UDT** section, view the **UDT Status**.

5 If the UDT status is **Enabled**, click **Disable UDT**.

When UDT is disabled, HTTP(S) is enabled.

6 If you want to enable data encryption for HTTPS transfer, see"Data Encryption," on page 64 and "Enabling Data Encryption for HTTP(S) Transfer Protocol," on page 64.

7 Log out of the node Admin Web console.

Data Encryption

You can choose whether data is encrypted during transfer.

If you are using the HTTP(s) protocol, which is the default protocol used by vCloud Connector for data transfer, data is encrypted by default. You can deselect or select data encryption by setting the **Disable SSL** or **Enable SSL** option on the destination vCloud Connector node. SSL is enabled on vCloud Connector nodes by default.

If you are using the UDT protocol, data is transferred as plain text by default. You can select data encryption by selecting the **Enable Encryption** option on the destination vCloud Connector node. Note that selecting this option is the only way to enable encryption with UDT. The SSL setting has no effect on UDT transfer; it only applies to HTTP(s) transfer.

You should be aware that there is some performance loss associated with encryption.

Enabling Data Encryption for HTTP(S) Transfer Protocol

When you use the HTTP(S) protocol for data transfer, data is encrypted by default, that is, HTTPS is used.

You can deselect or select data encryption by setting the **Disable SSL** or **Enable SSL** option in the vCloud Connector node. Set this option in the destination node. The SSL status on the destination node determines whether data transfer to the node is encrypted or unencrypted. However, when you copy data between a private cloud and a public cloud, the SSL status on the public cloud node determines whether data transfer is encrypted or unencrypted.

SSL is enabled by default on vCloud Connector nodes.

Prerequisites

The vCloud Connector node is configured to use HTTP(S) as the data transfer protocol. HTTP(S) is enabled whenever UDT is disabled.

Procedure

1 Go to the node Admin Web console at https://*vCCNodeIPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Verify that HTTP(S) is selected as the data transfer protocol.

a Click the **Node** tab, then click the **General** tab.

b Under **UDT**, verify that **UDT Status** displays **Disabled**.

HTTP(S) is enabled whenever UDT is disabled.

4 Click the **SSL** tab.

5 Click **Disable SSL** or **Enable SSL**.

6 Log out of the node Admin Web console.

What to do next

After you enable or disable SSL for a vCloud Connector node, you must update the node's registration with the vCloud Connector server.

Enabling Data Encryption for UDT Data Transfer Protocol

Data is not encrypted by default when the UDT protocol is used for data transfer. To encrypt data during UDT transfer, select the **Enable Encryption** option for UDT on the destination vCloud Connector node. If you are copying data between a private cloud and a public cloud, select the option on the vCloud Connector node in the public cloud.

When you copy data between two private clouds, the encryption status on the destination node determines whether UDT transfer to that node is encrypted or unencrypted. When you copy data between a private cloud and a public cloud, the encryption status on the public cloud node determines whether data transfer is encrypted or unencrypted.

NOTE The SSL setting on a node has no effect when UDT is selected as the data transfer protocol. To use encryption with UDT, you must select the **Enable Encryption** option.

Prerequisites

You have enabled UDT for the vCloud Connector node.

Procedure

1 Go to the node Admin Web console at https://*vCCNodeIPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Click the **Node** tab, then click the **General** tab.

4 Under **UDT**, verify that the **UDT Status** is **Enabled**.

5 Under **Encryption**, click **Enable Encryption**.

6 Log out of the node Admin Web console.

Set UDT Properties

You can set properties to configure the packet size of UDT packets and the buffer size for UDT in source or destination clouds.

You may need to configure UDT in some scenarios. For example, in low bandwidth networks, if you copy a large object from a private cloud to a public cloud using the UDT protocol, copy might fail. In this case, configure a smaller UDT packet size and update the buffer size accordingly.

You can set the following properties.

Table 7-2. UDT Properties

Property	Description	Default Value	Recommended Value
`udt_pkt_size`	Packet size of UDT packets	1048576 KB	For low bandwidth networks: 1024-1048576 (1KB to 1MB)
`udt_snd_buf_size`	Buffer size of UDT at the source	10485760 KB	Approximately 10 times `udt_pkt_size` The value must be greater than `udt_pkt_size`.
`udt_rcv_buf_size`	Buffer size of UDT at the destination	10485760 KB	Approximately 10 times `udt_pkt_size` The value must be greater than `udt_pkt_size`.

Set the properties in the source and destination vCloud Connector nodes.

Procedure

1 Log in to the node console as **`admin`**.

  The default password is **`vmware`**.

2 Change directories to `/usr/local/tcserver/vfabric-tc-server-standard/agent/webapps/agent/WEB-INF/spring/appServlet`.

3 Open the `management.xml` file in a text editor.

4 Search for `property name="udtProperties"`.

5 Edit the properties.

6 Save and close the file.

Using Proxy Servers

You can use proxy servers with both the HTTP(S) and UDT data transfer protocols.

Using a Proxy Server with UDT

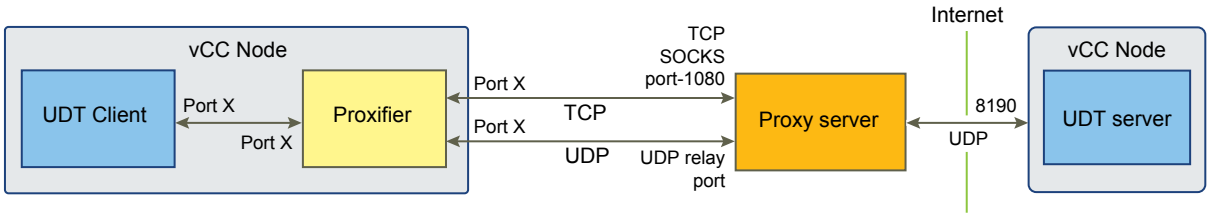
You can use UDT-based data transfer with SOCKS5-compliant proxy servers as these proxy servers support the UDP protocol. Note that you cannot use UDT-based data transfer with any other type of proxy server.

VMware recommends enabling encryption when you use a proxy server.

Communication between the node and the proxy server occurs with two separate connections: a TCP connection, to create the setup for UDT transfer, and a UDP connection for data transfer. Both connections are maintained until the data transfer is completed.

This communication between the node and the proxy server occurs over dynamically generated ports on the node and the following ports on the proxy server: the SOCKS port, which is usually 1080, for the TCP connection, and the UDP relay port for the UDP connection. Any firewall rules for the node should allow traffic from all ports to the proxy server, for both TCP and UDP protocols.

Figure 7-1. Using a Proxy Server with UDT



Procedure

1 Enable UDT on the source and destination nodes.

See "Select UDT Protocol for Data Transfer," on page 63.

2 Enable encryption for UDT transfer on the destination node.

See "Enabling Data Encryption for UDT Data Transfer Protocol," on page 65.

3 Specify proxy settings for UDT on the source node.

a Go to the node Admin Web console at https://*vCCNodeIPaddress*:5480.

b Log in as **`admin`**.

The default password is **`vmware`**.

c Click the **Node** tab, then click the **General** tab.

d In the **UDT Proxy** section, specify the proxy server options.

Option	Description
Proxy Server IP address	The IP address of the proxy server. For example, **`10.10.10.10`**.
Port	The SOCKS port.
Username	(Optional) The user name for the proxy server, if the proxy server requires authentication.
Password	(Optional) The password for the proxy server, if the proxy server requires authentication.

e Log out of the node Admin Web console.

When you copy data, vCloud Connector uses the proxy information to log in to the proxy server, do a handshake and create a UDT relay server on it, and transmit UDP traffic through the proxy server.

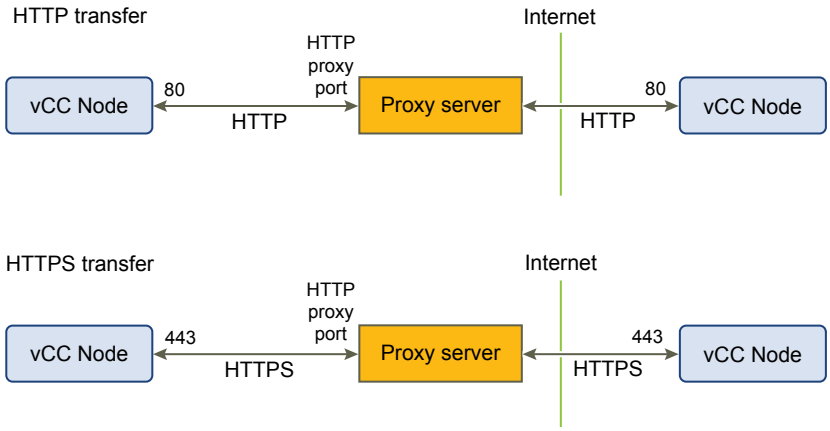
Using a Proxy Server with HTTP(S)

You can use HTTP(S)-based data transfer with proxy servers that you have set up in your environment.

VMware recommends enabling encryption when you use a proxy server.

Communication between the nodes and the proxy server occurs over standard ports: port 80 when SSL is disabled and port 443 when SSL is enabled.

Figure 7-2. Using a Proxy Server with HTTP(S)



Procedure

1 Enable HTTP(S) on the source and destination nodes.

See "Select HTTP(S) Protocol for Data Transfer," on page 64.

2 Enable encryption for HTTPS transfer on the destination node.

See "Enabling Data Encryption for HTTP(S) Transfer Protocol," on page 64.

3 Specify proxy settings on the source node.

a Go to the node Admin Web console at https://*vCCNodeIPaddress*:5480.

b Log in as **`admin`**.

The default password is **`vmware`**.

c Click the **Network** tab, then the **Proxy** tab.

d Select the **Use a proxy server** checkbox.

e Specify the proxy server options.

Option	Description
HTTP Proxy Server	The IP address of the proxy server. For example, **`10.10.10.10`**.
Proxy Port	The proxy port.
Proxy Username	(Optional) The user name for the proxy server, if the proxy server requires authentication. **NOTE** Specify a user name that contains lower-case, alpha-numeric characters only and does not exceed 50 characters. Do not use email addresses or domain names (for example, user@company.com or xyz\user) or names that contain a period (for example, firstname.lastname) as special characters are not supported for this field.
Proxy Password	(Optional) The password for the proxy server, if the proxy server requires authentication.

f Click **Save Settings**.

g Log out of the node Admin Web console.

Firewall Rules for UDT Copy Between Private and Public Clouds

You can set firewall rules for UDT copy between private and public clouds, or between two private networks separated by a firewall, if you do not want to use a proxy server.

Table 7-3. Firewall Rules for UDT Copy

Source	Port	Protocol	Destination	Port
Private Node	HTTPS any	TCP	Public Node	HTTPS 443
Private Node	HTTP any	TCP	Public Node	HTTP 80
Private Node	UDP any	UDP	Public Node	UDP 8190
Server	HTTPS any	TCP	Public Node	HTTPS 443
Server	HTTP any	TCP	Public Node	HTTP 80
Server	HTTPS any	TCP	Public Cloud	HTTPS 443
Server	HTTP any	TCP	Public Cloud	HTTP 80

NOTE If your environment has two firewalls between the source and destination vCloud Connector nodes, you cannot use the UDT protocol to copy data. UDT-based copy occurs over dynamically-generated ports on the source node and port 8190 on the destination node (or, when you copy between a private cloud and a public cloud, between a dynamically-generated port on the private cloud node and port 8190 on the public cloud node). Any firewall rules must allow for this type of connection for data transfer. In an environment with two firewalls, this connection is not possible.

Preparing vCloud Connector for Production Use

8

Before you place vCloud Connector into production use, you must prepare it for a full production environment.

Procedure

1 Add Valid SSL Certificates on page 71

If you have not yet replaced the self-signed certificates in your vCloud Connector server and vCloud Connector nodes, you need to do so before production use.

2 Upload Certificates from the Command Line on page 74

In some cases, you need to upload certificates from the command line.

3 Add CA Root Certificate to Trusted Keystore on page 75

When you add valid certificates and enable SSL for a vCloud Connector node, you must also import the corresponding Certificate Authority (CA) root certificate into the trusted keystore of the vCloud Connector server and all other vCloud Connector nodes.

4 Configure vCloud Connector Node Allocated Storage on page 76

Copy operations rely on staging storage when you copy resources between clouds. To successfully copy resources, make sure you have enough storage allocated to the vCloud Connector nodes.

5 Increase Maximum Concurrent Tasks on page 77

In vCloud Connector, you can start multiple tasks at the same time. By default, vCloud Connector executes a maximum of 10 concurrent tasks per vCloud Connector node, that is, per cloud. If you specify more than 10 tasks, the first 10 tasks are executed concurrently. When a task finishes, the next one in the queue is executed.

Add Valid SSL Certificates

If you have not yet replaced the self-signed certificates in your vCloud Connector server and vCloud Connector nodes, you need to do so before production use.

In a production environment, vCloud Connector requires root, intermediate, and signed certificates for the vCloud Connector server and nodes. All three certificates are required. The certificates must be in the X.509 format.

If your Certificate Authority (CA) only issues two certificates, you need to upload them from the command-line as the UI does not allow you to upload fewer than three certificates. See "Upload Certificates from the Command Line," on page 74 for more information.

Certificates are added to the `/usr/local/tcserver/vfabric-tc-server-standard/agent_or_server/conf/tcserver.jks` keystore.

When you add valid certificates and enable SSL for a node, you must also import the corresponding CA root certificate into the trusted keystore of the vCloud Connector server and all other vCloud Connector nodes. See "Add CA Root Certificate to Trusted Keystore," on page 75.

Procedure

1 Go to the Admin Web console of the vCloud Connector server or node at https://*vCCServer_or_Node_IPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 For vCloud Connector server, click the **Server** tab, then click the **SSL** tab. For vCloud Connector node, click the **Node** tab, then click the **SSL** tab.

4 Create a new private key if your Certificate Authority requires you to do so.

- To generate a 1024-bit key, complete these steps.

a In the **Generate New Key** section of the Manage SSL Certificates page, specify the following options.

Option	Description
Public key algorithm	The encryption algorithm: RSA or DSA
Public key size	The key size. From the UI, you can only generate a 1024-bit key. Use the command line to generate a 2048-bit key.
Common Name	The IP address or fully qualified domain name of the server or node. For example: **10.10.10.10** or **myNode.mycompany.com**
Organizational Unit	Your department name.
Organization	Your company name.
Locality	The city in which your company is based.
State	The state in which your company is based.
Country Code	The country in which your company is based.

b Click **Generate Key**.

- To generate a 2048-bit key, use the command line interface.

a Log in to the vCloud Connector server or node console as **admin**.

The default password is **vmware**.

b Change directory. For the server, change to this directory.

```
cd /usr/local/tcserver/vfabric-tc-server-standard/server/conf
```

For the node, change to this directory.

```
cd /usr/local/tcserver/vfabric-tc-server-standard/agent/conf
```

c Delete the existing key.

For the server, use this command.

```
/usr/java/default/bin/keytool -delete -alias hcserver -keystore tcserver.jks -
storepass changeme
```

For the node, use this command.

```
/usr/java/default/bin/keytool –delete –alias hcagent –keystore tcserver.jks –
storepass changeme
```

d Generate the new 2048-bit key.

For the server, use this command.

```
/usr/java/default/bin/keytool –genkey –keyalg RSA –keysize 2048 –alias hcserver –
validity 1095 –keystore tcserver.jks –storepass changeme –keypass changeme
```

For the node, use this command.

```
/usr/java/default/bin/keytool –genkey –keyalg RSA –keysize 2048 –alias hcagent –
validity 1095 –keystore tcserver.jks –storepass changeme –keypass changeme
```

e Log out of the console.

5 In the Admin Web console, click **Generate and download CSR** to generate a Certificate Signing Request and download it.

The vCloud Connector server file is named `hcserver.csr`. The vCloud Connector node file is named `hcagent.csr`.

6 Obtain certificates from your CA using the `.csr` files you downloaded.

NOTE If you are obtaining certificates from a Windows Server 2008 Certificate Authority, select the Subordinate Certificate Authority template type while requesting the certificate.

7 If the certificates you obtain from your CA are not in the X.509 format, convert them to the X.509 format by using the following command at the command prompt.

```
openssl pkcs7 –in <path/../certificate.cer> –print_certs | openssl x509 >
<path/../certificate.cer>
```

NOTE You must have the OpenSSL library installed to access this command. You can also use this command from the server or node console.

NOTE If the certificate is already in the X.509 format, you might get an error.

8 When you have your certificates in the X.509 format, upload them.

a In the **Root CA certificate** field, click **Browse** and find the root certificate for the vCloud Connector server or node.

b In the **Intermediate CA certificate** field, click **Browse** and find the intermediate certificate for the vCloud Connector server or node.

c In the **Certificate** field, click **Browse** and find the signed certificate for the vCloud Connector server or node.

d Click **Upload**.

9 Click **Enable SSL** at the top of the page.

NOTE You can ignore the following message: "vCloud Connector server hostname does not match CN in SSL certificate."

What to do next

After you install valid certificates, you must do the following.

- Deselect the **Ignore SSL Certificate** flag for each node for which you installed a valid certificate and update the node's registration with the vCloud Connector server.

  a Go to the vCloud Connector server Admin Web console at https://*vCCServer_IPaddress*:5480.

b Log in as **admin**. The default password is **vmware**.

c Click the **Nodes** tab.

d Click the gears icon next to the node and select **Edit**.

e Deselect **Ignore SSL Certificate**, then click **Update**.

See also "Register vCloud Connector Nodes with vCloud Connector Server," on page 49.

- Restart the vCloud Connector server after uploading new certificates for the change to take effect.

Upload Certificates from the Command Line

In some cases, you need to upload certificates from the command line.

The vCloud Connector server and vCloud Connector node Admin Web consoles support uploading only a single root, intermediate, and signed certificate. To upload multiple root or intermediate certificates, use the command line interface.

Also use the command line interface if you need to upload fewer than three certificates as the UI requires you to upload all three certificates. Some Certificate Authorities only issue two certificates.

Certificates must be in the X.509 format.

You must import certificates in the following order: root certificate, intermediate certificate, then signed certificate.

NOTE If you obtain certificates from a Windows Server 2008 Certificate Authority, ensure that you select the Subordinate Certificate Authority template type while requesting the certificate.

Prerequisites

You have obtained the certificates and have copied them to a directory in the vCloud Connector server or node.

Procedure

1 Log in to the console of the vCloud Connector server or vCloud Connector node as **admin**.

The default password is **vmware**.

2 If the certificates that you obtained from your Certificate Authority are not in the X.509 format, convert them to the X.509 format.

```
openssl pkcs7 –in <path/../certificate.cer> –print_certs | openssl x509 >
<path/../certificate.cer>
```

NOTE If the certificate is already in the X.509 format, you might get an error.

---

3 At the prompt, change directory.

```
cd /usr/local/tcserver/vfabric–tc–server–standard/server_or_agent/conf
```

4 Import the root certificate.

```
/usr/java/default/bin/keytool –import –trustcacerts –alias root –file <location of root .cer
file> –keystore tcserver.jks –storepass changeme
```

5 Import intermediate certificates. Ensure that you import multiple intermediate certificates in an order of signing chain.

```
/usr/java/default/bin/keytool -import -trustcacerts -alias intermediate -file <location of intermediate .cer file> -keystore tcserver.jks -storepass changeme
```

NOTE You must provide a unique alias name for every intermediate certificate you upload.

6 Import the signed certificate.

```
/usr/java/default/bin/keytool -import -trustcacerts -alias hcserver_or_hcagent -file <location of .cer file> -keystore tcserver.jks -storepass changeme
```

7 Enable SSL.

a Go to the server or node Admin Web console at https://*vCCServer_or_Node_IPaddress*:5480.

b Log in as **admin**.

The default password is **vmware**.

c For the server, click the **Server** tab, then click the **SSL** tab. For the node, click the **Node** tab, then click the **SSL** tab.

d Click **Enable SSL**.

NOTE You can ignore the following message: "vCloud Connector server hostname does not match CN in SSL certificate."

What to do next

After you install valid certificates, you must do the following.

- Deselect the **Ignore SSL Certificate** flag for each node for which you installed a valid certificate and update the node's registration with the vCloud Connector server.

  a Go to the vCloud Connector server Admin Web console at https://*vCCServerIPaddress*:5480.

  b Log in as **admin**. The default password is **vmware**.

  c Click the **Nodes** tab.

  d Click the gears icon next to the node and select **Edit**.

  e Deselect **Ignore SSL Certificate**, then click **Update**.

  See also "Register vCloud Connector Nodes with vCloud Connector Server," on page 49.

- Restart the vCloud Connector server after uploading new certificates for the change to take effect.

Add CA Root Certificate to Trusted Keystore

When you add valid certificates and enable SSL for a vCloud Connector node, you must also import the corresponding Certificate Authority (CA) root certificate into the trusted keystore of the vCloud Connector server and all other vCloud Connector nodes.

The trusted keystore is `/usr/java/default/lib/security/cacerts`. The default password for this keystore is **changeit**.

Procedure

1 Log in to the console of the vCloud Connector server or vCloud Connector node as **admin**.

The default password is `vmware`.

2 If the CA Root certificate is not in the X.509 format, convert it to the X.509 format.

```
openssl pkcs7 –in <path/../certificate.cer> –print_certs | openssl x509 >
<path/../certificate.cer>
```

NOTE If the certificate is already in the X.509 format, you might get an error.

3 At the prompt, change directory.

```
cd /usr/java/default/lib/security
```

4 Import the root certificate.

```
/usr/java/default/bin/keytool –import –trustcacerts –alias alias –file <location of root .cer
file> –keystore cacerts –storepass changeit
```

Ensure that all root certificates uploaded to the `cacerts` keystore have a unique alias name.

Configure vCloud Connector Node Allocated Storage

Copy operations rely on staging storage when you copy resources between clouds. To successfully copy resources, make sure you have enough storage allocated to the vCloud Connector nodes.

Default storage on vCloud Connector nodes is 40 GB. You may need to increase this in some cases.

- If you will be copying large virtual machines, vApps, or templates.

  In some scenarios (for example, if the transfer or import part of the copy process is slower than the export), vCloud Connector uses the staging area during copy and might need storage equivalent to the size of the object being copied.
- If you will be copying many items simultaneously from a cloud.
- If you increase the maximum number of concurrent copies allowed for a node.

Configure vCloud Connector Node Allocated Storage in vSphere

To successfully copy resources to or from a vSphere cloud, you must configure and resize the data disk associated with the vCloud Connector node for that vSphere cloud.

Prerequisites

- You are a vSphere administrator.
- You have taken a snapshot of the virtual appliance.

Procedure

1 Log in to the vSphere Client.

2 In the hierarchy tree, select the vCloud Connector node virtual appliance.

3 Right-click and select **Edit Settings**.

The **Virtual Machine Properties** window opens to the **Hardware** tab.

4 Select **Hard disk 2** in the **Hardware** column.

5 Modify the size, based on the size of the resources you are going to be transferring, and click **OK**.

6 Open the console for the vCloud Connector node.

7 Run the following command to resize the disk:

```
sudo /opt/vmware/hcagent/scripts/resize_disk.sh
```

Configure vCloud Connector Node Allocated Storage in vCloud Director

To successfully copy resources to or from a vCloud Director cloud, you must add disk storage to the vCloud Connector node associated with that cloud.

To add disk storage in vCloud Director, you must add disks.

Prerequisites

You are a vCloud Director organization administrator. You are logged in to vCloud Director.

Procedure

1 Power off the vCloud Connector node.

2 Click the **My Cloud** tab.

3 Select **VMs** in the left panel.

4 Right-click the console icon of the powered-down vCloud Connector node in the center panel and select **Properties**.

5 In the Virtual Machine Properties dialog box, click the **Hardware** tab.

6 Click the **+ Add** button to add an additional disk to the node.

7 Size the disk based on the size of the resources you intend to transfer and click **OK**.

8 Right-click the node console icon and power on the node.

9 Right-click the node console icon and select **Popout Console**.

If you have not yet installed the VMware Remote Console plug-in, you are prompted to install it.

If the node is still powering on, wait for the log in screen to appear.

10 Log in to the node as **`admin`**.

The default password is **`vmware`**.

11 At the command prompt, type: `ls /dev/sd*`

The new disk has a name such as "sdc".

12 Run the following command to add the new disk.

```
sudo /opt/vmware/hcagent/scripts/add_disk.sh <diskname>
```

13 Log out of the console.

Increase Maximum Concurrent Tasks

In vCloud Connector, you can start multiple tasks at the same time. By default, vCloud Connector executes a maximum of 10 concurrent tasks per vCloud Connector node, that is, per cloud. If you specify more than 10 tasks, the first 10 tasks are executed concurrently. When a task finishes, the next one in the queue is executed.

You can increase the maximum number of concurrent tasks for a vCloud Connector node.

If you increase the maximum number of concurrent tasks, you should also increase the storage allocated to the node accordingly. The amount of extra storage you need depends upon the size of the resources you intend to transfer. About 50 GB is recommended for each added task.

As most tasks, such as a copy task, involve both a source cloud and a destination cloud, the maximum number applies to both. If you increase the maximum so that you can execute more than 10 copies at a time, for example, increase the storage for the node in both the source and destination cloud.

Procedure

1 Go to the vCloud Connector node Admin Web console at https://*vCCNodeIPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Click the **Node** tab, then click the **General** tab.

4 In the **Concurrent Tasks Configuration** section, type the maximum number of concurrent tasks, then click **Change Maximum Concurrent Tasks**.

5 Log out of the vCloud Connector node Admin Web console.

What to do next

Increase the storage allocated for the vCloud Connector node. See "Configure vCloud Connector Node Allocated Storage," on page 76.

Cross-Cloud Data Transfer and Network Connectivity

9

vCloud Connector manages the transfer of content using a separate component, the vCloud Connector node. This flow affects the way a request moves through the system and how network connectivity must be set up.

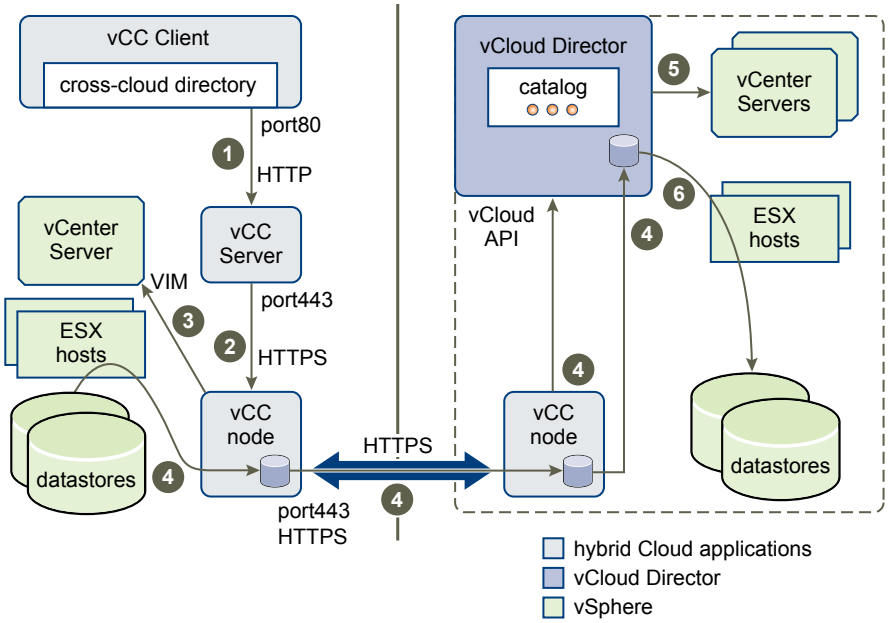
Data Flow in Transfer

The following figure shows the path a vCloud Connector request takes in transferring data from a vSphere to a vCloud Director (VCD) cloud.

NOTE This figure depicts default settings. Port 443 is used when SSL is enabled and port 80 is used when SSL is disabled. By default, SSL is disabled for the vCloud Connector server and enabled for vCloud Connector nodes.

Enabling or disabling SSL on the vCloud Connector server affects communication from the vCloud Connector UI to the server. Enabling or disabling SSL on vCloud Connector nodes affects communication from the server to the nodes and communication between nodes.

Figure 9-1. Cross-cloud Data Flow



1 Customer requests transfer using vCloud Connector UI.

2 vCloud Connector server tells vCloud Connector node to transfer vApp.

3 Node tells vCenter Server to export using VIM API.

4 Export begins and the following tasks happen in parallel because data is streamed.

- Content is moved from datastores to source node cache.
- Content is transferred from source to destination node.
- Destination node calls the VCD API to import.
- Content transfers from destination node cache to VCD transfer server storage.

5 VCD sends the command for the appropriate vCenter import.

6 Content transfers from VCD transfer server storage to destination datastore network and is made available through the VCD catalog.

Uninstalling vCloud Connector 10

To uninstall vCloud Connector, delete the vCloud Connector server and all the vCloud Connector nodes associated with it. Before you delete the server, you must unregister it from the vSphere Client to which it is registered. Before you delete a node, you must unregister it from the server to which it is registered.

This chapter includes the following topics:

Uninstall a vCloud Connector Server

To uninstall vCloud Connector, unregister and delete the vCloud Connector server and vCloud Connector nodes.

Procedure

1 Go to the vCloud Connector server Admin Web console at https://*vccServerIPaddress*:5480.

You can get the IP address of the vCloud Connector server from its console in the vSphere Client or vCloud Director cloud in which it is installed.

2 Log in as **admin**.

If you did not change the password, use **vmware**, the default password.

3 Unregister the vCloud Connector nodes that are registered with the vCloud Connector server.

a Click the **Nodes** tab.

b Click the gears icon next to the first cloud and select **Unregister** from the pop-up menu.

c Click **OK** to confirm.

d Repeat for all the clouds that are registered with the server.

4 Unregister the vCloud Connector server from the vSphere client to which it is registered.

a Click the **Server** tab, then click the **vSphere Client** tab.

b Type the user name and password for the vSphere Client.

c Click **Unregister**.

5 Remove the server from the vSphere or vCloud Director cloud in which it is installed.

To remove the server from a vSphere Client, complete these steps.

a Log in to the vSphere Client.

b In the Inventory pane, select **VMs and Templates**.

c Find your vCloud Connector server virtual machine in the tree view.

d Right-click your vCloud Connector server virtual machine and select **Power > Power Off** from the pop-up menu.

e When the vCloud Connector server virtual machine is powered off, right-click it again and select **Delete from Disk** from the pop-up menu.

To remove the server from a vCloud Director cloud, complete these steps.

a Log in to the vCloud Director cloud.

b Click the **My Cloud** tab.

c In the My Cloud panel, select **vApps**.

d Find your vCloud Connector server vApp in the Name column, right-click it, and select **Stop** from the pop-up menu.

e When the Status column displays **Stopped** for the vCloud Connector server vApp, right-click it again and select **Delete** from the pop-up menu.

f Click **Yes** to confirm.

The vCloud Connector server is now deleted. You cannot access vCloud Connector from the vSphere Client.

Uninstall vCloud Connector Nodes

You can uninstall a vCloud Connector node from a cloud if you no longer want to transfer content to and from that cloud. You must also uninstall vCloud Connector nodes when you uninstall vCloud Connector.

Procedure

1 Go to the vCloud Connector server Admin Web console at https://*vccServerIPaddress*:5480.

You can get the IP address of the vCloud Connector server from its console in the vSphere Client or vCloud Director cloud in which it is installed.

2 Log in as **`admin`**.

If you did not change the password, use **`vmware`**, the default password.

3 Click the **Nodes** tab.

4 Click the gears icon next to the vCloud Connector node to delete, then select **Unregister** from the pop-up menu.

The node is now unregistered from the server.

5 Repeat Step 4 for all the nodes you want to delete. If you are uninstalling vCloud Connector, delete all the nodes that are registered with the server.

6 Log in to the cloud in which the vCloud Connector node is installed.

7 If the node is installed on a vSphere cloud, delete it from the cloud.

a In the **Inventory** pane, select **VMs and Templates**.

b In the tree view, right-click the vCloud Connector node virtual machine and select **Power > Power Off** from the pop-up menu.

c When the vCloud Connector node virtual machine is powered off, right-click it again and select **Delete from Disk** from the pop-up menu.

8 If the vCloud Connector node is installed on a vCloud Director cloud, delete it from the cloud.

   a Click the **My Cloud** tab.

   b In the My Cloud panel, select **vApps**.

   c Find your vCloud Connector node vApp in the Name column, right-click it, and select **Stop** from the pop-up menu.

   d When the Status column shows **Stopped** for the vCloud Connector node vApp, right-click it again and select **Delete** from the pop-up menu.

   e Click **Yes** to confirm.

The vCloud Connector node is deleted from the cloud. The cloud does not appear in the list of clouds in the vCloud Connector UI.

11 Upgrading to vCloud Connector 2.5

To upgrade to vCloud Connector 2.5, follow the upgrade process described here. Note that you can only upgrade from version 2.0 to 2.5; you cannot upgrade from earlier versions to 2.5.

NOTE After you upgrade vCloud Connector, clear your Internet Explorer browser cache before you use the upgraded version. You need to do this to ensure new data is shown in the vCloud Connector server and node Admin Web consoles and in the UI.

This chapter includes the following topics:

Use the Admin Web Console to Upgrade to vCloud Connector 2.5

To upgrade to vCloud Connector 2.5, you upgrade your vCloud Connector server and all vCloud Connector nodes. You upgrade a vCloud Connector server or node from its Admin Web console.

NOTE You can upgrade only from vCloud Connector 2.0 to 2.5. You cannot upgrade from earlier versions.

Prerequisites

Verify that you have the IP address of the vCloud Connector server or node. You can get the IP address from its console in the vSphere cloud or vCloud Director cloud in which it is installed.

Procedure

1. Go to the vCloud Connector server or node Admin Web console at https://*vCCServerIPaddress*:5480 or https://*vCCNodeIPaddress*:5480.
2. Log in as **admin**.

   The default password is **vmware**.
3. Click the **Update** tab, and click the **Status** tab.
4. Click **Check Updates**.

   The available updates appear.
5. Click **Install Updates**.
6. Accept the EULA.
7. Click **OK** in the confirmation dialog box and wait for the update process to finish.
8. Click the **System** tab.

9 Click **Reboot**.

You are logged out of the Admin Web console when the system finishes rebooting.

Update Registration with vSphere Client

After you upgrade the vCloud Connector server and nodes, you must update the registration of the vCloud Connector UI with the vSphere Client.

If you do not update the registration, vCloud Connector does not appear in the Solutions and Applications panel on the **Home** tab in vSphere Client.

Prerequisites

You have upgraded your vCloud Connector 2.0 server and nodes to version 2.5.

Procedure

1 Go to the vCloud Connector server Admin Web console at https://*vCCServerIPaddress*:5480.

You can get the IP address of the vCloud Connector server from its console in the vSphere cloud or vCloud Director cloud in which it is installed.

2 Log in as **`admin`**.

The default password is **`vmware`**.

3 Click the **Server** tab, then click the **vSphere Client** tab.

4 Specify the vCenter user name and password, then click **Update Registration**.

5 Log out of the server Admin Web console.

What to do next

Before you use the upgraded version of vCloud Connector, clear your Internet Explorer browser cache.

Enter a license key if you want to use vCloud Connector 2.5 Advanced edition. See Chapter 4, "Entering the License Key for vCloud Connector Advanced Edition," on page 53.

Troubleshooting vCloud Connector 12

Use this information to troubleshoot problems with your vCloud Connector installation.

Troubleshooting Storage

If a transfer is interrupted in the middle, for example because of a network outage, temporary storage in the node might not be cleaned up, leading to a loss of usable storage space, even if the transfer completes normally.

If you notice that the available storage space in a node has decreased after a transfer that was interrupted, reboot the node. The temporary files are deleted on reboot.

Troubleshooting Connectivity

You can use cURL to pinpoint connectivity problems among the components of your vCloud Connector installation.

Log in to the appropriate instance as **admin** either through the console or with SSH. The default password is **vmware**. The following procedure tests all the connections in order. Use whichever segments are useful to you. Use the -x, --proxy <[protocol://]proxyhost> option if necessary.

Prerequisites

You have installed your vCloud Connector server and nodes and they are powered on. You have any necessary proxy information.

Procedure

1 Log in to the vCloud Connector server to test the server connections.

2 Test the connection between the vCloud Connector server and a vCloud Director cloud.

```
curl –k –v https://vcd–host/api/versions
```

3 Test the connection between the vCloud Connector server and a vCenter Server.

```
curl –k –v https://vc–host/mob
```

4 Test the connection between the vCloud Connector server and a vCloud Connector node.

```
curl –k –v https://node–host/agent/api/v2/org/org/version
```

5 Log in to the vCloud Connector node located in the vSphere internal cloud to test the node connections used in the copy path.

6 Test the connection between the vCloud Connector node and the vCenter Server.

```
curl –k –v https://vc–host/mob
```

7 Test the connection between the vCloud Connector node and the ESX host.

```
curl –k –v https://esx–host/mob
```

8 Test the connection between the vSphere vCC node and a vCloud Director vCC node outside the firewall.

```
curl –k –v https://node–host/agent/api/v2/org/org/version
```

9 Log in to the vCloud Director vCC node.

10 Test the connection between the vCloud Director vCC node and the vCloud Director cloud.

```
curl –k –v https://vcd–host/api/versions
```

Accessing Log Files from the UI

You can access log files for a vCloud Connector server or vCloud Connector node instance from its Admin Web console.

NOTE If you are using a public cloud, you can only access your own log files, not those of other organizations in the cloud.

NOTE If you are using a multi-tenant vCloud Connector node deployed by a public vCloud service provider or private vCloud Director system administrator, you do not have access to the Node Admin Web console. See "Accessing Log Files for Multi-tenant Nodes," on page 60.

Procedure

1 Go to the vCloud Connector server or vCloud Connector node Admin Web console at https://*Server_or_Node_IPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Download the log files.

- In the server Admin Web console, click the **Server** tab, then click the **General** tab and click **Download logs**.
- In the node Admin Web console, click the **Node** tab, then click the **General** tab and click **Download logs**.

4 Save the zip file.

5 Extract files from the zip file.

The node log file is named hca.log and is in the `opt/vmware/hcagent/logs` directory. The server log file is named hcs.log and is in the `opt/vmware/hcserver/logs` directory.

Older log files are in a zip file in the same directory.

Tomcat log files are named **catalina.*Date*.log**.

Accessing Log Files from the Console

You can access log files for a vCloud Connector server or vCloud Connector node instance through its console.

Server log files are in the `/opt/vmware/hcserver/logs` directory. Node log files are in the `/opt/vmware/hcagent/logs` directory.

Node log files are divided by organization.

NOTE If you are using a public cloud, you can only access your own log files, not those of other organizations in the cloud.

NOTE If you are using a multi-tenant vCloud Connector node deployed by a public vCloud service provider or private vCloud Director system administrator, you do not have access to the node console. See "Accessing Log Files for Multi-tenant Nodes," on page 60.

Procedure

1 In your vSphere Client or vCloud Director cloud, open the server or node console and log in as **admin**.

The default password is **vmware**.

2 Change directory.

- In the server console, go to the `/opt/vmware/hcserver/logs` directory.

```
cd /opt/vmware/hcserver/logs
```

- In the node console, go to the `/opt/vmware/hcagent/logs` directory.

```
cd /opt/vmware/hcagent/logs
```

3 View the hcs.log file (for vCloud Connector server) or hca.log file (for vCloud Connector node).

Older log files are in a zip file in the same directory.

For vCloud Connector nodes, organization-specific log files are in **/opt/vmware/hcagent/logs/*Organization*/**.

Tomcat log files are named **catalina.*Date*.log**.

Accessing Log Files for Multi-tenant Nodes

If you are using a vCloud Connector node that has been deployed as a multi-tenant node by a public vCloud service provider or private vCloud Director system administrator, you do not have access to the vCloud Connector node console or Admin Web console. You can download node log files for your own organization from your vCloud Connector server Admin Web console.

Procedure

1 Go to your vCloud Connector server Admin Web console at https://*vCCServerIPaddress*:5480.

2 Log in as **admin**.

The default password is **vmware**.

3 Click the **Nodes** tab.

4 Click the gears icon next to the multi-tenant node that you registered with your server, and select **Download Logs**.

5 Save the zip file.

6 Extract files from the zip file.

The node log file is named hca.log and is in the `opt/vmware/hcagent/logs` directory.

Troubleshooting Log File Size

To modify the size of log files or the number of files that are retained, you must modify the vCloud Connector server or node configuration files.

Prerequisites

The original configuration file is backed up.

Procedure

1 Open the server or node console and log in as **admin**.

The default password is **vmware**.

2 For vCloud Connector server, navigate to `/usr/local/tcserver/vfabric-tc-server-standard/server/webapps/hcserver/WEB-INF/classes/logback.xml`.

3 For vCloud Connector node, navigate to `/usr/local/tcserver/vfabric-tc-server-standard/agent/webapps/agent/WEB-INF/classes/logback.xml`

4 Adjust the appropriate values in the following XML sections.

```
<rollingPolicy class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
     <fileNamePattern>/opt/vmware/hcserver or hcagent/logs/hcs.%i.log.zip or hca.
%i.log.zip</fileNamePattern>
     <minIndex>1</minIndex>
     <maxIndex>9</maxIndex>
 </rollingPolicy>

<triggeringPolicy class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
     <maxFileSize>10MB</maxFileSize>
</triggeringPolicy>
```

To modify the number of files to retain, change `rollingPolicy/maxIndex` to the desired number.

To modify the size of log files, change `triggeringPolicy/maxFileSize` to the desired size.

NOTE This is the size of a single file, so the total log size could be as large as this value times the maxNumber value. Archived log files are zipped, however, so the total log size is usually much smaller.

5 Save the file. You do not need to restart.

Using Fully Qualified Domain Names (FQDNs)

You can use FQDNs for the vCloud Connector server and vCloud Connector nodes.

If you use FQDNs, you must use FQDNs that have proper entries in the DNS server so that the FQDNs get resolved to the correct address.

Index