Installing and Configuring vCloud Connector

vCloud Connector 2.6.0

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.
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:

doctorbackground@vmware.com
Contents

Installing and Configuring vCloud Connector 5

1 vCloud Connector Overview 7
   About vCloud Connector 7
   Planning Your vCloud Connector Installation 8

2 Installing vCloud Connector 11
   Collect Necessary Information 12
   System Requirements 14
   Deployment Considerations 16
   Download the vCloud Connector Virtual Appliances 16
   Install vCloud Connector Server 17
   Configure vCloud Connector Server 28
   Install vCloud Connector Nodes 31
   Register vCloud Connector Nodes with Clouds 43
   Configure vCloud Connector Nodes 44
   Register vCloud Connector Nodes with vCloud Connector Server 49
   Register the vCloud Connector UI 50

3 Deploying Multitenant Nodes as a vCloud Service Provider 53

4 Using Service Provider Multitenant Nodes 57
   Use Service Provider Nodes 57
   Use vCloud Hybrid Service Multitenant Nodes 58
   Accessing Log Files for Multitenant Nodes 60

5 Selecting Copy Options 61
   About vCloud Connector Copy 61
   Compatibility with Earlier Versions of vCloud Connector 62
   Data Transfer Protocols for Copy 62
   Data Encryption 64
   Set UDT Properties 66
   Using Proxy Servers 66
   Firewall Rules for Copying Between Private and Public Clouds 69
   Copying Large Virtual Machines or vApps 69

6 Preparing vCloud Connector for Production Use 71
   Add Valid SSL Certificates 71
   Upload Certificates from the Command Line 74
   Add CA Root Certificate to Trusted Keystore 75
   Configure vCloud Connector Node Allocated Storage 76
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. This information is written for cloud system administrators who are familiar with VMware vSphere®, VMware vSphere® Client™, and VMware vCloud Director®, and with deploying virtual appliances. To use the Datacenter Extension feature, you should also be familiar with VMware vCloud® Networking and Security™ and with networking concepts.
vCloud Connector Overview

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:
- “About vCloud Connector,” on page 7
- “Planning Your vCloud Connector Installation,” on page 8

About 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 manage virtual machines, deploy templates, and transfer virtual machines, vApps, and templates from one cloud to another.

vCloud Connector also provides the following key features.
- Content Sync lets you set up a Content Library to distribute and synchronize templates across clouds.
- Datacenter Extension (Stretch Deploy) lets you extend your private data center to a public vCloud.
- Offline Data Transfer enables you to transfer large amounts of data from your private data center to vCloud Hybrid Service.

vCloud Connector Components

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

The vCloud Connector UI is the user interface that the vCloud Connector server produces. It is registered to and accessed from the vSphere Client. You decide where to register 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. You only need one vCloud Connector server.

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 vCloud Director-based clouds, the service provider can install a vCloud Connector node as a multitenant node for multiple customers to use so that each customer does not have to install a node. This configuration can also be used by private vCloud Director administrators who have multiple organizations.

In vCloud Hybrid Service, a vCloud Connector multitenant node is installed by VMware by default.

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 multitenant, 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.

To add a vCloud Hybrid Service cloud instance to the vCloud Connector UI, you do not need to install a node in vCloud Hybrid Service. You use the multitenant node that is installed by default by VMware.

- Which vSphere Client you want to use for the vCloud Connector 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 12.
Installing vCloud Connector is a multi-step process. This section gives you a high-level overview of the steps you need to take.

Figure 2-1. 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 multitenant node. To connect a vCloud Hybrid Service cloud instance, you use the vCloud Connector multitenant node that is installed by VMware.

You only need one vCloud Connector server for your installation.

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 do 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.

Connect a private vSphere or vCloud Director cloud with vCloud Hybrid Service.

**Procedure**

1. **Collect Necessary Information** on page 12
   Print this worksheet section to help you collect the information you need to install and configure vCloud Connector.

2. **System Requirements** on page 14
   You must ensure that your system meets the minimum requirements before you install vCloud Connector.

3. **Deployment Considerations** on page 16
   When you install vCloud Connector, consider these requirements.

4. **Download the vCloud Connector Virtual Appliances** on page 16
   The vCloud Connector server and vCloud Connector node are packaged as virtual appliances. You download the virtual appliances from the vCloud Connector Download page.

5. **Install vCloud Connector Server** on page 17
   You can install a vCloud Connector server in a vSphere cloud or in a vCloud Director cloud.

6. **Configure vCloud Connector Server** on page 28
   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.

7. **Install vCloud Connector Nodes** on page 31
   You can install vCloud Connector nodes in vSphere or vCloud Director clouds.

8. **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.

9. **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.

10. **Register vCloud Connector Nodes with vCloud Connector Server** on page 49
    After you install a vCloud Connector server and nodes, you use the server Admin Web console to register the nodes with the server. The nodes can be installed on vSphere, private vCloud Director clouds, public vClouds, or vCloud Hybrid Service. The registration allows the server to manage the nodes.

11. **Register the vCloud Connector UI** on page 50
    To surface 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 2-1. Account Information

<table>
<thead>
<tr>
<th>Account Type</th>
<th>Information Needed</th>
<th>Used For</th>
</tr>
</thead>
<tbody>
<tr>
<td>One of the following:</td>
<td>User name, password, and URL or IP address for the appropriate entity</td>
<td>Installing vCloud Connector server</td>
</tr>
<tr>
<td>■ VMware® vCenter Server™ administrator account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>■ VMware vCloud Director® account with at least organization administrator status</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

vCenter Server administrator account for each vSphere cloud

<table>
<thead>
<tr>
<th>Information Needed</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name, password, and URL or IP address</td>
<td>Installing vCloud Connector node</td>
</tr>
</tbody>
</table>

vCloud Director account with at least organization administrator status for each vCloud Director cloud

<table>
<thead>
<tr>
<th>Information Needed</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name, password, and URL or IP address</td>
<td>Installing vCloud Connector node</td>
</tr>
</tbody>
</table>

vCenter Server administrator account or any account that has Extension privileges for the vCenter Server in which you want to use the vCloud Connector UI

<table>
<thead>
<tr>
<th>Information Needed</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name, password, and FQDN or IP address</td>
<td>Registering the vCloud Connector UI</td>
</tr>
</tbody>
</table>

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 type of proxy server.

Proxy Servers

You need the following proxy information.

Table 2-2. Proxy Information

<table>
<thead>
<tr>
<th>Install Type</th>
<th>Information Needed</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Connector server host:port</td>
<td>If the server needs a proxy to be able to access systems beyond the firewall in the location in which it is installed.</td>
<td></td>
</tr>
<tr>
<td>User name and password, if the proxy server requires authentication. See “Network Tab (Server),” on page 29 for user name restrictions.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

vCloud Connector node - per node host:port

<table>
<thead>
<tr>
<th>Information Needed</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name and password, if the proxy server requires authentication. See “Network Tab (Node),” on page 45 for user name restrictions.</td>
<td>If the node needs a proxy to be able to access systems beyond the firewall in the location in which it is installed.</td>
</tr>
</tbody>
</table>
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 2-3. Network Information

<table>
<thead>
<tr>
<th>Network Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>An available static IP address</td>
</tr>
<tr>
<td>The netmask for that address</td>
</tr>
<tr>
<td>The IP address of the gateway</td>
</tr>
<tr>
<td>The IP address of a primary and secondary DNS server</td>
</tr>
<tr>
<td>A host name (optional)</td>
</tr>
</tbody>
</table>

For information on network paths in data transfers, see Chapter 7, “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 2-4. vCloud Connector UI in vSphere

<table>
<thead>
<tr>
<th>vCloud Connector UI in vSphere</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address or fully qualified domain name of the vCenter Server to which you will be connecting.</td>
</tr>
<tr>
<td>A user name and password for the vCenter Server. Use a vCenter server administrator role or any role that includes Extension privileges.</td>
</tr>
<tr>
<td>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.</td>
</tr>
</tbody>
</table>

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

Hardware Requirements
The vCloud Connector UI is registered as a plug-in in vSphere Client. To use the vSphere Client, you must have a Windows machine, with Internet Explorer installed. For more information on systems requirements for the vSphere Client, see the VMware vSphere documentation.

Software Requirements
To install and configure a vCloud Connector server and nodes, you need to install the following VMware products.
Table 2.5. VMware Products

<table>
<thead>
<tr>
<th>Product</th>
<th>Supported Version</th>
<th>Notes</th>
</tr>
</thead>
</table>
| 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. |
| 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 for the vCloud Connector UI. 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 2.6. Supported Browsers

<table>
<thead>
<tr>
<th>Browser</th>
<th>Supported Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>8, 9</td>
</tr>
<tr>
<td>Chrome</td>
<td>22, 23</td>
</tr>
</tbody>
</table>

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 2.7. Port Information

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>Used when SSL is enabled. This port is used for communication between the vCloud Connector server and vCloud Connector nodes and between nodes.</td>
</tr>
<tr>
<td>80</td>
<td>Used when SSL is disabled. This port is used for communication between the vCloud Connector server and vCloud Connector nodes and between nodes.</td>
</tr>
</tbody>
</table>
Table 2-7. Port Information (Continued)

<table>
<thead>
<tr>
<th>Port Number</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>8190</td>
<td>Required on the destination node for UDT-based data transfer. <strong>Note</strong> When you copy data between a private cloud and a public cloud, port 8190 needs to be open on the public cloud.</td>
</tr>
<tr>
<td>5480</td>
<td>This port is used for communication with the vCC server and vCC node Admin Web consoles.</td>
</tr>
</tbody>
</table>

**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.

See also Chapter 7, “Cross-Cloud Data Transfer and Network Connectivity,” on page 79.

**Load Balancers**

If there is a load balancer between a vCloud Connector node and the cloud with which it is associated, the load balancer should have session persistence enabled.

**Deployment Considerations**

When you install vCloud Connector, consider these requirements.

- For each cloud that you add to vCloud Connector, the vCloud Connector server must be able to reach the following.
  - The vCloud Connector node associated with the cloud
  - The cloud
    The vCloud Connector server accesses the cloud directly to get its inventory and for tasks such as powering on or powering off virtual machines or vApps. It accesses the cloud through the public API.
  - If there is a load balancer between a vCloud Connector node and the cloud with which it is associated, the load balancer should have session persistence enabled.
  - For the list of ports vCloud Connector uses, see “System Requirements,” on page 14.
  - For information about deploying multitenant nodes as a service provider, see Chapter 3, “Deploying Multitenant Nodes as a vCloud Service Provider,” on page 53.

**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 12.

**Procedure**

1. Go to the vCloud Connector Download page.
2. Click Download Now.
3 Scroll down to the **Product Downloads** section and download both the vCCServer and vCCNode zip files.
   a Click either **Download** or **Download Manager**.
      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 18.

**Prerequisites**

You must have an administrator account for the vSphere instance in which you want to 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 16.

**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 28.

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 19
   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 19
   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.
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 16.

**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.

**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 20.

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 “**System Requirements,**” on page 14 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 Specify Any for the source IP address and the source port.

12 Type the destination IP address and port.

The destination IP address is the external IP address.

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 22

   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 22

   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 23

   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 16.

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.

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 23.

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 “System Requirements,” on page 14 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 want to NAT all ports, enter * for the first port entry.
   
   If you want 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 Click **Add SNAT**.

   The Add Source NAT Rule dialog box appears.

12 Select the network on which to apply the rule.

13 Specify the internal IP address that is assigned to the vCloud Connector server.

14 Specify the External (Translated) IP address that all outgoing traffic has to go through.

15 Click **OK**.

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

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

   The Add Firewall Rule popup appears.

   Create a rule for each required port.

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

19 Give the rule a name.

20 Unless specified, type **Any** in the **Source IP Address** text box and **Any** in the **Source Port** text box.

21 Type the destination IP address and port.

   The destination IP address is the external IP address.

22 Select the protocol.

23 Select **Allow**.

24 Click **OK** 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 25
   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 26
   After the vCloud Connector server is added to the vCloud Director 5.5 cloud as a vApp 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 26
   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 16.

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 This may take several seconds after the upload itself has finished for the process to be finalized.
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 vApp 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 vCloud Connector 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, an optional description, and the virtual data center in which to store the vApp, then click **Next**.
4. Select the storage policy for the virtual machine, and click **Next**.
5. Select the 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.
6. Select the IP allocation from the IP allocation drop-down menu, and click **Next**.
7. In the Networking Properties page, specify the netmask, IP address, DNS server, and default gateway information, and click **Next**.
   If you are using DHCP, you can leave these fields blank.
8. Customize hardware settings, if needed, and click **Next**.
9. Review your settings and click **Finish**.
10. Click the **My Cloud** tab, then select **vApps** in the My Cloud panel on the left.
    You can see the vApp being created.
11. Select **VMs** in the My Cloud panel, right-click your vCloud Connector server virtual machine, and select **Properties**.
12. In the Virtual Machine Properties dialog box, click the **Guest OS Customization** tab, select **Enable guest customization**, and click **OK**.
13. In the My Cloud panel, select **vApps**, then right-click your vCloud Connector server vApp and select **Start**.
14. 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 want 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 “System Requirements,” on page 14 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. Select the network on which to apply the rule.
8. Specify the external IP address.
9. If you want to NAT all ports, select ANY for the Original port entry.
   If you want to NAT only the required ports, create a rule for each port.
10. Specify the translated (internal) IP address from your initial setup and match the port entry for this rule.
11. Click OK.
12. Click Add SNAT.
   The Add Source NAT Rule dialog box appears.
13. Select the network on which to apply the rule.
14. Specify the internal IP address that is assigned to the vCloud Connector server.
15. Specify the External (Translated) IP address that all outgoing traffic has to go through.
16. Click OK.
17. If you are using a firewall rule to control traffic, click the Firewall tab and select the Enable firewall check box.
18. Click Add at the bottom of the page to create a new firewall rule.
   Create a rule for each required port.
19. Select the Enabled check-box, if it is not already selected.
20. Give the rule a name.
21. Unless specified, type Any in the Source IP Address text box and Any in the Source Port text box.
22. Type the destination IP address and port.
   The destination IP address is the external IP address.
23. Select the protocol.
24. Select Allow.
25. 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 12.

**Procedure**

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 12 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 12.

For more information about network paths in data transfers, see Chapter 7, “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.

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

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

Server Tab

In the **Server** tab, the **General** and **SSL** tabs allow you to change the server administrator password, adjust log levels, and manage SSL certificates. The **vSphere Client** tab is used later in the registration process to register the UI.

General

The **General Settings** section allows you to change the administrator password for the vCloud Connector server, 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. |
| 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 hserver.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>
<thead>
<tr>
<th>Table 2-8. Options</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Task</strong></td>
</tr>
<tr>
<td>To register a node with the server</td>
</tr>
<tr>
<td>To edit a node's registration</td>
</tr>
<tr>
<td>To unregister a node from the server</td>
</tr>
<tr>
<td>To download node log files</td>
</tr>
<tr>
<td>To specify Stretch Deploy settings</td>
</tr>
<tr>
<td>To unregister Stretch Deploy settings</td>
</tr>
</tbody>
</table>

### Install vCloud Connector Nodes

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

You must install a 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 multitenant node installed by the service provider.

As vCloud Connector does not require every organization in a vCloud Director cloud to install its own node, public vCloud service providers or administrators of private vCloud Director clouds can install a node in the cloud as a multitenant node for multiple customers to use. See Chapter 3, “Deploying Multitenant Nodes as a vCloud Service Provider,” on page 53 for more information.

To use a multitenant 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.

See also “Deployment Considerations,” on page 16.
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 18.

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 16.

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 16.
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 multitenant 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 multitenant 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 3, “Deploying Multitenant Nodes as a vCloud Service Provider,” on page 53 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 multitenant node.
- If a multitenant 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 multitenant 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 33
   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 34
   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 35
   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 16.

**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.

### 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 35.

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 “System Requirements,” on page 14 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.
   The Add Firewall Rule popup appears.
   Create a rule for each necessary port.
10. Give the rule a name and select the Incoming option.
11. Specify Any for the source IP address and the source port.
12. Type the destination IP address and port.
   The destination IP address is the external IP address.
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 multitenant 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 multitenant 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 3, “Deploying Multitenant Nodes as a vCloud Service Provider,” on page 53 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 multitenant node.
- If a multitenant 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 multitenant 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 36

   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 37

   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 38

   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.
Click **Catalogs**.

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

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

Click the **Upload** icon.

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

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

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

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.

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 38.

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 want 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 “System Requirements,” on page 14 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 want to NAT all ports, enter * for the first port entry.

If you want 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 Click **Add SNAT**.
   The Add Source NAT Rule dialog box appears.
12 Select the network on which to apply the rule.
13 Specify the internal IP address that is assigned to the vCloud Connector node.
14 Specify the External (Translated) IP address that all outgoing traffic has to go through.
15 Click **OK**.
16 If you are using a firewall rule to control traffic, click the **Firewall** tab and select the **Enable firewall** check box.
17 Click **Add** at the bottom of the page to create a new firewall rule.
   The Add Firewall Rule dialog box appears.
   Create a rule for each required port.
18 Select the **Enabled** check-box.
19 Give the rule a name.
20 Unless specified, type **Any** in the **Source IP Address** text box and **Any** in the **Source Port** text box.
21 Type the destination IP address and port.
   The destination IP address is the external IP address.
22 Select the protocol.
23 Select **Allow**.
24 Click **OK** 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 multitenant 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 multitenant 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 3, “Deploying Multitenant Nodes as a vCloud Service Provider,” on page 53 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 multitenant node.
If a multitenant 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 multitenant 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 40
   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 41
   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 16.

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.

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, an optional description, and the virtual data center in which to store the vApp, then click Next.
4. Select the storage policy for the virtual machine, and click Next.
5. Select the 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.
6. Select the IP allocation from the IP allocation drop-down menu, and click Next.
7. In the Networking Properties page, specify the netmask, IP address, DNS server, and default gateway information, and click Next. If you are using DHCP, you can leave these fields blank.
8. Customize hardware settings, if needed, and click Next.
9. Review your settings and click Finish.
10. Click the My Cloud tab, then select vApps in the My Cloud panel on the left. You can see the vApp being created.
11. Select VMs in the My Cloud panel, right-click your vCloud Connector node virtual machine, and select Properties.
12. In the Virtual Machine Properties dialog box, click the Guest OS Customization tab, select Enable guest customization, and click OK.
13. In the My Cloud panel, select vApps, then right-click your vCloud Connector node vApp and select Start.
14. 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 want 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 “System Requirements,” on page 14 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. Select the network on which to apply the rule.
8. Specify the external IP address.
9. If you want to NAT all ports, select ANY for the Original port entry.
   If you want to NAT only the required ports, create a rule for each port.
10. Specify the translated (internal) IP address from your initial setup and match the port entry for this rule.
11. Click OK.
12. Click Add SNAT.
   The Add Source NAT Rule dialog box appears.
13. Select the network on which to apply the rule.
14. Specify the internal IP address that is assigned to the vCloud Connector node.
15. Specify the External (Translated) IP address that all outgoing traffic has to go through.
16. Click OK.
17. If you are using a firewall rule to control traffic, click the Firewall tab and select the Enable firewall check box.
18. Click Add at the bottom of the page to create a new firewall rule.
   Create a rule for each required port.
19. Select the Enabled check-box, if it is not already selected.
20. Give the rule a name.
21. Unless specified, type Any in the Source IP Address text box and Any in the Source Port text box.
22. Type the destination IP address and port.
   The destination IP address is the external IP address.
23 Select the protocol.

24 Select Allow.

25 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 multitenant 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


   NOTE Do not use Firefox as some tabs display blank pages in Firefox.

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://10.10.10.10
   - 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 multitenant 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 12.

**Procedure**

2. If you receive a certificate warning, accept the certificate.
3. Log in as **admin**.
   
   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 12.

For more information about network paths in data transfers, see Chapter 7, “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.

<table>
<thead>
<tr>
<th>To check for updates automatically</th>
<th>Select Automatic check for updates, then set the frequency for the update check.</th>
</tr>
</thead>
<tbody>
<tr>
<td>To check for updates and install the updates automatically</td>
<td>Select Automatic check and install updates, then select the frequency for the update check.</td>
</tr>
<tr>
<td>To deselect automatic update settings</td>
<td>Select No automatic updates.</td>
</tr>
<tr>
<td>To update from the default repository</td>
<td>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.</td>
</tr>
<tr>
<td>To update from a CDROM</td>
<td>Select Use CDROM Updates.</td>
</tr>
<tr>
<td>To update from a specific repository</td>
<td>Select Use Specified Repository and type the user name and password for the repository, if required.</td>
</tr>
</tbody>
</table>

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 multitenant node for use by multiple organizations, this task is performed by the service provider or network administrator of the cloud.

<table>
<thead>
<tr>
<th>Cloud Type</th>
<th>The type of cloud.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud URL</td>
<td>The URL of the cloud. You can specify either the IP address of the cloud or its fully qualified domain name (FQDN):</td>
</tr>
<tr>
<td></td>
<td><strong><a href="https://CloudIPaddress">https://CloudIPaddress</a></strong></td>
</tr>
<tr>
<td></td>
<td>For example: <strong><a href="https://10.10.100.10">https://10.10.100.10</a></strong></td>
</tr>
<tr>
<td></td>
<td><strong><a href="https://CloudFQDN">https://CloudFQDN</a></strong></td>
</tr>
<tr>
<td></td>
<td>For example: <strong><a href="https://cloud1.company.com">https://cloud1.company.com</a></strong></td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Ignore SSL Cert</td>
<td>Select this option if the cloud does not have a valid SSL certificate. <strong>Note:</strong> 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.</td>
</tr>
<tr>
<td>Use Proxy</td>
<td>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 <strong>Network - Proxy</strong> tab.</td>
</tr>
</tbody>
</table>

**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.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change admin user password</td>
<td>Specify a new administrator password for the vCloud Connector node, then click <strong>Confirm new password</strong>. You should change the default password.</td>
</tr>
<tr>
<td>Log levels</td>
<td>Set the severity level for vCloud Connector node log files, then click <strong>Change log level</strong>.</td>
</tr>
<tr>
<td>Download logs</td>
<td>Click to download a zip file of vCloud Connector node log files. <strong>Note:</strong> If you are using a multitenant 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.</td>
</tr>
<tr>
<td>Concurrent Tasks</td>
<td>Specify the maximum number of concurrent tasks that are allowed for the vCloud Connector node, then click <strong>Change Maximum Concurrent Tasks</strong>. 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.</td>
</tr>
<tr>
<td>UDT</td>
<td>UDT is a data transfer protocol that can be used instead of HTTP(S) to copy data. <strong>UDT Status</strong> displays whether UDT is currently enabled or disabled for the node. Select <strong>Enable UDT</strong> or <strong>Disable UDT</strong> to enable or disable UDT. When UDT is disabled, HTTP(S) is used to copy data. <strong>Note:</strong> You must select the <strong>Enable UDT</strong> option on both the source and destination nodes. If UDT is enabled on only one of the nodes, HTTP(S) is used. See Chapter 5, “Selecting Copy Options,” on page 61 for more information.</td>
</tr>
</tbody>
</table>

*Disclaimer: The information in this document is subject to change without notice. VMware, Inc. is not responsible for typographical errors or omissions.*
### UDT Proxy

Specify information about the proxy server that you want to use with UDT data transfer, then click Configure UDT Proxy.

<table>
<thead>
<tr>
<th><strong>Proxy Server IP address</strong></th>
<th>The IP address of the proxy server. For example, <strong>10.10.10.10</strong>.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Port</strong></td>
<td>The SOCKS port.</td>
</tr>
<tr>
<td><strong>Username</strong></td>
<td>(Optional) The user name for the proxy server, if the proxy server requires authentication.</td>
</tr>
<tr>
<td><strong>Password</strong></td>
<td>(Optional) The password for the proxy server, if the proxy server requires authentication.</td>
</tr>
</tbody>
</table>

**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

After you install a vCloud Connector server and nodes, you use the server Admin Web console to register the nodes with the server. The nodes can be installed on vSphere, private vCloud Director clouds, public vClouds, or vCloud Hybrid Service. 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 multitenant node deployed on a public vCloud or private vCloud Director cloud, get the node URL from the service provider or cloud administrator. To register a multitenant node deployed in vCloud Hybrid Service, get the node URL from VMware Support.

Procedure

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

   **NOTE** Do not use Firefox as some tabs display blank pages in Firefox.

2. Log in to the Web console as `admin`.
   The default password is `vmware`.

3. Click the **Nodes** tab.
   The Manage Nodes page lists all the vCloud Connector nodes that are currently registered with the server.
   The Local Content Library 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.

<table>
<thead>
<tr>
<th>Node Details Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Display Name</strong></td>
<td>A name for the cloud. The cloud will appear by this name in the vCloud Connector UI.</td>
</tr>
<tr>
<td><strong>Node URL</strong></td>
<td>The URL of the node. You can specify either the IP address of the node or its FQDN.</td>
</tr>
<tr>
<td></td>
<td>- <a href="https://vCCNodeIPaddress">https://vCCNodeIPaddress</a></td>
</tr>
<tr>
<td></td>
<td>For example: <a href="https://10.10.100.10">https://10.10.100.10</a></td>
</tr>
<tr>
<td></td>
<td>- <a href="https://FQDN">https://FQDN</a></td>
</tr>
<tr>
<td></td>
<td>For example: <a href="https://node1.company.com">https://node1.company.com</a></td>
</tr>
</tbody>
</table>

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 this option if the cloud is a public cloud outside the firewall where your vCloud Connector server is installed. |
Node Details Option | Description
---|---
Use Proxy | Select this option if your vCloud Connector server needs to use a proxy to reach the node that you are registering.
Ignore SSL Certificate | Select this option 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 Credentials 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) The name of your organization in the vCloud Director cloud, for example, MyOrg.
**Note**: You must use a valid organization name. vCloud Connector validates the name that you provide with the cloud.
If you selected vSphere in the Cloud Type option, this field is disabled.
**Note**: If you are registering a service provider multitenant node, specify the name of your organization in the public cloud. If you are registering a vCloud Hybrid Service multitenant node, specify the name of your virtual data center in vCloud Hybrid Service. See Chapter 4, “Using Service Provider Multitenant Nodes,” on page 57 for more information.
Username | User name for the cloud.
Password | Password for the cloud.

7 Click Register.

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 for the node.

**Note**: Do not update or unregister a vCloud Connector node while a task is in progress.

Register the vCloud Connector UI

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

Register the vCloud Connector UI in vSphere Client

The vCloud Connector UI appears as a plug-in in vSphere Client. Use the vCloud Connector server Admin Web console to register the vCloud Connector UI with the vSphere Client.

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** If you are overwriting a registration, clear your Internet Explorer cache before you register. Also clear the Internet Explorer cache if you have unregistered and are registering again. Ensure that the **Preserve Favorites Website** data option is deselected in the Delete Browsing History dialog box when you clear the cache.

**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 12. You need the IP address of the vCloud Connector server. You need the IP address or fully qualified domain name of the vCenter Server to which the vSphere Client is pointed. You also need an administrator account, or any user role that has Extension privileges, for the vCenter Server.

**Procedure**


   **Note** Do not use Firefox as some tabs appear blank in Firefox.

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.

   For example, https://10.10.10.10.

   If you are using DHCP, this field is automatically filled.

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

   For example, 10.10.10.10.

   **Note** If your vCenter Server is running on a port other than the default, ensure that you specify the port number with the IP address.

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

8. If the vCenter server has a vCloud Connector server already registered with it that you want to replace, select **Overwrite existing registration**.

9. If the vCloud Connector server needs to go through a proxy server to reach the vCenter server, select **Use Proxy**.

   If you select **Use Proxy**, ensure that you have specified proxy settings in the **Network** tab.

10. 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 page. To verify that the vCloud Connector UI appears in vSphere Client, log in to the vSphere Client and check that the vCloud Connector icon appears under **Solutions and Applications** in the **Home** page.
Deploying Multitenant Nodes as a vCloud Service Provider

vCloud Connector nodes are multitenant, 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 multitenant 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.

- Multitenant Node A for customers 1-20 on public vCloud 1
- Multitenant Node B for customers 21-40 on public vCloud 1
• Multitenant Node C for customers 41-60 on public vCloud 2
• Multitenant 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 multitenant node is dedicated to a group of customers, vCloud Connector does not support using a load balancer in front of a multitenant node.

• Customers' vCloud Connector servers must be able to reach the following.
  • The multitenant node
  • The cloud

  The vCloud Connector server accesses the cloud directly to get the inventory and for tasks such as powering on or powering off virtual machines and vApps. It accesses the cloud through the vCloud Director API.

• Each multitenant node can support up to 20 organizations.

• Check whether your customers want to use HTTPS or UDT as the data transfer protocol for copy. The default protocol is HTTP(S). To use UDT, both the source and destination nodes must have UDT enabled. If UDT is enabled on only one of the nodes, for example, if it is enabled on the multitenant node and not on the customer’s node, then HTTP(S) is used.

Note that the multitenant node must be registered with a customer’s server before you can select the Enable UDT option for the multitenant node. UDT cannot be enabled on a node until the node is registered with a server.

For more information, see Chapter 5, “Selecting Copy Options,” on page 61.

• If you use UDT, and if the multitenant node is being accessed by a public FQDN, ensure that its hostname is set to the public FQDN.

Deploying Multitenant Nodes

1 Determine how many multitenant nodes you need based on the number of customers you intend to support.
   Each node can support 20 organizations.

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

   Note: You do not need to install a vCloud Connector server in the public cloud.

3 Set NAT and firewall rules as specified below.

4 Add valid SSL certificates to the nodes. See “Add Valid SSL Certificates,” on page 71 for information.
   If you add a valid certificate and enable SSL, customers need to import the corresponding CA root certificate into the trusted keystore of their server and nodes. See “Add CA Root Certificate to Trusted Keystore,” on page 75 for information.

5 Increase the node staging area. See “Configure vCloud Connector Node Allocated Storage,” on page 76 for information.

   Note: If you use NFS share to increase the staging area, use the no-lock option for mounting the NFS share.
6 If you are planning to use UDT, and if the multitenant node is going to be accessed by a public FQDN, ensure that the node's hostname is set to the public FQDN.
   a Log in to the multitenant node's Admin Web console at https://nodeIP:5480, set the public FQDN as the hostname in the Network - Address tab, and click Save Settings.
   b Log in to the multitenant node's console.
   c Change to root.
      
      su root
      
      The default password is vmware.
   d Add the following line to the /etc/hosts file.
      multitenantNodeInternalIP multitenantNodeFQDN
   e Restart the network service.
      service network restart

7 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

Also inform customers whether the multitenant node has a valid certificate and has SSL enabled so that they can select the appropriate settings while registering the node.

8 Ask 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.

9 Enable UDT on the node, if required.

   Each customer will register the multitenant 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.

Firewall and NAT Rules

For an on-premise vCloud Connector server and node to reach the multitenant node in the public cloud, you need to set NAT and firewall rules in the public cloud.

Set these rules.
   ■ Open port 443 for HTTPS traffic.
   ■ Open port 80 for HTTP traffic.
   ■ Open port 8190 for UDT traffic, if you enable UDT on the multitenant node.

**NOTE** If these ports are in use, you can use a different port for the original (outbound) port.

**NOTE** Do not open port 5480, which is used to access the node Admin Web console. As a service provider, you configure the multitenant node before you provide the node URL to your customers.
### Table 3-1. Sample NAT Rule for Multitenant Node

<table>
<thead>
<tr>
<th>Rule</th>
<th>Original IP</th>
<th>Port</th>
<th>Translated IP</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNAT</td>
<td>Public IP</td>
<td>443</td>
<td>Private IP of node</td>
<td>443</td>
<td>TCP</td>
</tr>
<tr>
<td>DNAT</td>
<td>Public IP</td>
<td>80</td>
<td>Private IP of node</td>
<td>80</td>
<td>TCP</td>
</tr>
<tr>
<td>DNAT</td>
<td>Public IP</td>
<td>8190</td>
<td>Private IP of node</td>
<td>8190</td>
<td>UDP</td>
</tr>
<tr>
<td>SNAT</td>
<td>Private IP of node</td>
<td>Any</td>
<td>Public IP</td>
<td>Any</td>
<td>Any</td>
</tr>
</tbody>
</table>

### Table 3-2. Sample Firewall Rule for Multitenant Node

<table>
<thead>
<tr>
<th>Source</th>
<th>Port</th>
<th>Destination</th>
<th>Port</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any</td>
<td>Any</td>
<td>Public IP</td>
<td>443, 80</td>
<td>TCP</td>
</tr>
<tr>
<td>Any</td>
<td>Any</td>
<td>Public IP</td>
<td>8190</td>
<td>UDP</td>
</tr>
<tr>
<td>Private IP of node</td>
<td>Any</td>
<td>Any</td>
<td>443, 80</td>
<td>TCP</td>
</tr>
<tr>
<td>Private IP of node</td>
<td>Any</td>
<td>Any</td>
<td>8190</td>
<td>UDP</td>
</tr>
</tbody>
</table>

### Accessing Multitenant Node Log Files

As the multitenant 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 93 and “Accessing Log Files from the UI,” on page 92 for more information.

Customers do not have access to the multitenant 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 Multitenant Nodes,” on page 60 for more information.

### Upgrading a Multitenant Node

To upgrade a multitenant node, follow the process described in Chapter 9, “Upgrading to vCloud Connector 2.6,” on page 85. After you upgrade a multitenant node, customers who have registered the node with their vCloud Connector servers need to reload the cloud in the vCloud Connector UI.
To add a public cloud to your vCloud Connector installation, you can use the multitenant vCloud Connector node deployed by the service provider in the public cloud. You register the multitenant 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,” on page 57
- “Use vCloud Hybrid Service Multitenant Nodes,” on page 58
- “Accessing Log Files for Multitenant Nodes,” on page 60

### 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 multitenant node. To use a service provider node, ask your service provider to install a multitenant 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 Multitenant Nodes,” on page 58.

### Prerequisites

The service provider has installed a vCloud Connector node in the public cloud as a multitenant node.

### Procedure

1. Obtain the URL of the multitenant node deployed on the public cloud from your service provider.
2. Register the multitenant 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.
3. If the service provider has installed a valid SSL certificate on the multitenant node, import the corresponding CA root certificate into the trusted keystore of your vCloud Connector server and nodes.
   
   See “Add CA Root Certificate to Trusted Keystore,” on page 75.
Use vCloud Hybrid Service Multitenant Nodes

You can connect a vCloud Hybrid Service cloud instance to your vCloud Connector installation by using the multitenant vCloud Connector node that is deployed by VMware in vCloud Hybrid Service.

- “Register the vCloud Hybrid Service Multitenant Node,” on page 58
- “Add a Catalog in vCloud Hybrid Service,” on page 59

Register the vCloud Hybrid Service Multitenant Node

To connect a vCloud Hybrid Service cloud to your vCloud Connector installation, ask your service provider to install a multitenant vCloud Connector node in vCloud Hybrid Service and send you the node URL. You can then register the multitenant 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 individually with your vCloud Connector server. You do this by registering the multitenant 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 multitenant vCloud Connector node has been installed in vCloud Hybrid Service.

Procedure

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


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.

<table>
<thead>
<tr>
<th>Node Info Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A name for the cloud. The cloud will appear by this name in the vCloud Connector UI.</td>
</tr>
<tr>
<td>Description</td>
<td>A description of the vCloud Connector node.</td>
</tr>
</tbody>
</table>
To copy virtual machines, vApps, or templates to vCloud Hybrid Service, you must first add a catalog in 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 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 Click 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 Multitenant Nodes

If you are using a vCloud Connector node that has been deployed as a multitenant node by a public vCloud service provider or private vCloud Director system administrator, you do not have access to the node console or Admin Web console. You can download log files for the node, for your organization only, 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 multitenant 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.
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,” on page 61
- “Compatibility with Earlier Versions of vCloud Connector,” on page 62
- “Data Transfer Protocols for Copy,” on page 62
- “Data Encryption,” on page 64
- “Set UDT Properties,” on page 66
- “Using Proxy Servers,” on page 66
- “Firewall Rules for Copying Between Private and Public Clouds,” on page 69
- “Copying Large Virtual Machines or vApps,” on page 69

About vCloud Connector Copy

vCloud Connector includes a path-optimized copy mechanism that provides a relatively 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.

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.
Compatibility with Earlier Versions of vCloud Connector

The path-optimized copy mechanism, which was introduced in vCloud Connector 2.5, 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>
<thead>
<tr>
<th>Node A Version</th>
<th>Node B Version</th>
<th>Copy Mechanism Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.5 or later</td>
<td>2.5 or later</td>
<td>Path-optimized copy</td>
</tr>
<tr>
<td>2.5 or later</td>
<td>2.0</td>
<td>Old, 2.0 copy mechanism</td>
</tr>
<tr>
<td>2.0</td>
<td>2.5 or later</td>
<td>Old, 2.0 copy mechanism</td>
</tr>
<tr>
<td>2.0</td>
<td>2.0</td>
<td>Old, 2.0 copy mechanism</td>
</tr>
</tbody>
</table>

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 multitenant 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 and later, it can be used only if both the source and destination nodes are version 2.5 or later. 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**

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**

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

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.
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>
<thead>
<tr>
<th>Table 5-2. UDT Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
</tr>
<tr>
<td>----------</td>
</tr>
<tr>
<td>udt_pkt_size</td>
</tr>
<tr>
<td>udt_snd_buf_size</td>
</tr>
<tr>
<td>udt_rcv_buf_size</td>
</tr>
</tbody>
</table>

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.


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 5-1. Using a Proxy Server with UDT**

![Diagram of UDT with Proxy Server](image)

**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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy Server IP address</td>
<td>The IP address of the proxy server. For example, <strong>10.10.10.10</strong>.</td>
</tr>
<tr>
<td>Port</td>
<td>The SOCKS port.</td>
</tr>
<tr>
<td>Username</td>
<td>(Optional) The user name for the proxy server, if the proxy server requires authentication.</td>
</tr>
<tr>
<td>Password</td>
<td>(Optional) The password for the proxy server, if the proxy server requires authentication.</td>
</tr>
</tbody>
</table>

   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.
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.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Proxy Server</td>
<td>The IP address of the proxy server. For example, 10.10.10.10.</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>The proxy port.</td>
</tr>
<tr>
<td>Proxy Username</td>
<td>(Optional) The user name for the proxy server, if the proxy server requires</td>
</tr>
<tr>
<td></td>
<td>authentication. Note: Specify a user name that contains lower-case, alpha-</td>
</tr>
<tr>
<td></td>
<td>numeric characters only and does not exceed 50 characters. Do not use email</td>
</tr>
<tr>
<td></td>
<td>addresses or domain names (for example, <a href="mailto:user@company.com">user@company.com</a> or xyz\user) or</td>
</tr>
<tr>
<td></td>
<td>names that contain a period (for example, firstname.lastname) as special</td>
</tr>
<tr>
<td></td>
<td>characters are not supported for this field.</td>
</tr>
<tr>
<td>Proxy Password</td>
<td>(Optional) The password for the proxy server, if the proxy server requires</td>
</tr>
</tbody>
</table>

   f. Click Save Settings.
   g. Log out of the node Admin Web console.
Firewall Rules for Copying Between Private and Public Clouds

You can set firewall rules for copying 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>
<thead>
<tr>
<th>Table 5-3. Firewall Rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Protocol</td>
</tr>
<tr>
<td>Destination</td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Private Node</td>
</tr>
<tr>
<td>HTTPS any</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>Public Node</td>
</tr>
<tr>
<td>HTTPS 443</td>
</tr>
<tr>
<td>Private Node</td>
</tr>
<tr>
<td>HTTP any</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>Public Node</td>
</tr>
<tr>
<td>HTTP 80</td>
</tr>
<tr>
<td>Private Node</td>
</tr>
<tr>
<td>UDP any</td>
</tr>
<tr>
<td>UDP</td>
</tr>
<tr>
<td>Public Node</td>
</tr>
<tr>
<td>UDP 8190</td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>HTTPS any</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>Public Node</td>
</tr>
<tr>
<td>HTTPS 443</td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>HTTP any</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>Public Node</td>
</tr>
<tr>
<td>HTTP 80</td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>HTTPS any</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>Public Cloud</td>
</tr>
<tr>
<td>HTTPS 443</td>
</tr>
<tr>
<td>Server</td>
</tr>
<tr>
<td>HTTP any</td>
</tr>
<tr>
<td>TCP</td>
</tr>
<tr>
<td>Public Cloud</td>
</tr>
<tr>
<td>HTTP 80</td>
</tr>
</tbody>
</table>

**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.

Copying Large Virtual Machines or vApps

Copying large virtual machines or vApps with vCloud Connector can take several hours, depending on the size of the object you are copying and on the network.

To copy data to vCloud Hybrid Service, use the following guidelines.

<table>
<thead>
<tr>
<th>Size of VM or vApp</th>
<th>Recommended Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; 300 GB</td>
<td>Use the vCloud Connector Copy command.</td>
</tr>
<tr>
<td>&gt;300 GB</td>
<td>Use the Offline Data Transfer service.</td>
</tr>
</tbody>
</table>

To copy large virtual machines or vApps over a low bandwidth network with the vCloud Connector Copy command, configure your source and destination vCloud Connector nodes with the following settings. If you are copying to vCloud Hybrid Service, configure your on-premise node with these settings.

1. Log in to the node as **admin**. The default password is **vmware**.
2. Stop the tomcat service.
   
   ```bash
   /usr/local/tcsrvr/vfabric-tc-server-standard/agent/bin/tcruntime-ctl.sh stop
   ```
4. Open the `task.xml` file for editing.
Replace the following section, between lines 57-64,

```xml
<!-- Quartz job that physically deletes Task resources after a period of time -->
<bean id="removeOldTasksJob"
class="com.vmware.hc.agent.jobs.RemoveOldTasksJob"
init-method="initializeSchedule" lazy-init="false">
<property name="jobExecutionIntervalInHours" value="4"/>
<property name="taskCleanupIntervalInHours" value="48"/>
</bean>
```

with the following lines.

```xml
<!-- Quartz job that physically deletes Task resources after a period of time -->
<bean id="removeOldTasksJob"
class="com.vmware.hc.agent.jobs.RemoveOldTasksJob"
init-method="initializeSchedule" lazy-init="false">
<property name="jobExecutionIntervalInHours" value="24"/>
<property name="taskCleanupIntervalInHours" value="720"/>
</bean>
```

Start the tomcat service.

```
/usr/local/tcserver/vfabric-tc-server-standard/agent/bin/tcruntime-ctl.sh start
```
Preparing vCloud Connector for Production Use

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

This chapter includes the following topics:
- “Add Valid SSL Certificates,” on page 71
- “Upload Certificates from the Command Line,” on page 74
- “Add CA Root Certificate to Trusted Keystore,” on page 75
- “Configure vCloud Connector Node Allocated Storage,” on page 76
- “Increase Maximum Concurrent Tasks,” on page 77

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, upload both.

NOTE If you are obtaining certificates from a Windows Server 2008 Certificate Authority, select the Web Server template while requesting the certificate. Ensure that the Issuer field contains an Organization value. If there is no Organization value in the certificate, you might get an error while selecting the SSL option.

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.
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.

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.

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

  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.

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

  For the node, change to this directory.

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

  c. Delete the existing key.

  For the server, use this command.

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

  For the node, use this command.

    ```bash
/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.

    ```bash
/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.

    ```bash
/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 Web Server template while requesting the certificate. Ensure that the Issuer field contains an Organization value. If there is no Organization value in the certificate, you might get an error while selecting the SSL option.

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.

```bash
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 select the root certificate for the vCloud Connector server or node.

b In the **Intermediate CA certificate** field, click **Browse** and select the intermediate certificate for the vCloud Connector server or node.

c In the **Certificate** field, click **Browse** and select 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.
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.

Certificates must be in the X.509 format.

You must import certificates in the following order: root certificate, intermediate certificate, then signed certificate.

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 for information.

Prerequisites

You have obtained the certificates and have copied them to a directory in the vCloud Connector server or node.

Note If you are obtaining certificates from a Windows Server 2008 Certificate Authority, select the Web Server template while requesting the certificate. Ensure that the Issuer field contains an Organization value. If there is no Organization value in the certificate, you might get an error while selecting the SSL option.

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.
   ```plaintext
   /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.

**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/jre/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 Copy the certificate to a directory in the console.
3 If the CA Root certificate is not in the X.509 format, convert it to the X.509 format.
   ```plaintext
   openssl pkcs7 -in <path to certificate.cer> -print_certs | openssl x509 > <path to certificate.cer>
   ```

   **NOTE** If the certificate is already in the X.509 format, you might get an error.
4 Change directory.
   ```plaintext
   cd /usr/java/default/jre/lib/security
   ```
5 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.

6 Restart the server or node.

**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 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 have vSphere administrator privileges.
- Backing up the virtual appliance is recommended.

**NOTE** Do not take a snapshot as hard disks of appliances that have snapshots cannot be resized. Use another backup method such as creating a clone.

**Procedure**

1 Log in to the vSphere Client.

2 In the Home page, select **VMs and Templates**.

3 In the hierarchy tree, select the vCloud Connector node virtual appliance.

4 Right-click and select **Edit Settings**.

   The **Virtual Machine Properties** window opens to the **Hardware** tab.

5 Select **Hard disk 2** in the **Hardware** column.

6 Modify the size, based on the size of the resources you are going to be transferring, and click **OK**.

7 Right-click the vCloud Connector node virtual appliance and select **Open Console**.

8 Log in to the console as **admin** user.

   The default password is **vmware**.

9 Run the following command to resize the disk:

```
sudo /opt/vmware/hcagent/scripts/resize_disk.sh
```

   You will be prompted for the root password. The default password is **vmware**.
Type exit to log out of the console.

**Configure vCloud Connector Node 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 add disks.

**Prerequisites**

You have vCloud Director organization administrator privileges.

**Procedure**

1. In vCloud Director, click the **My Cloud** tab.
2. In the **My Cloud** pane on the left, select **VMs**.
3. In the **Virtual Machines** list, find the vCloud Connector node, right-click, and select **Power Off** to power off the node.
4. Right-click the vCloud Connector node and select **Properties**.
5. In the Virtual Machine Properties dialog box, click the **Hardware** tab.
6. Under **Hard Disks**, 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 and select **Power On** to power on the node.
9. Right-click the node 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.

   ```bash
   sudo /opt/vmware/hcagent/scripts/add_disk.sh <diskname>
   ```

   You will be prompted for the root password. The default password is **vmware**.
13. Type exit to 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**

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

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.

**Figure 7-1. 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

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,” on page 81
- “Uninstall vCloud Connector Nodes,” on page 82

Uninstall a vCloud Connector Server

To uninstall vCloud Connector, unregister and delete the vCloud Connector server and vCloud Connector nodes.

Procedure

   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.
Find your vCloud Connector server virtual machine in the tree view.

Right-click your vCloud Connector server virtual machine and select **Power > Power Off** from the pop-up menu.

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.

- Log in to the vCloud Director cloud.
- Click the **My Cloud** tab.
- In the My Cloud panel, select **vApps**.
- Find your vCloud Connector server vApp in the Name column, right-click it, and select **Stop** from the pop-up menu.
- When the Status column displays **Stopped** for the vCloud Connector server vApp, right-click it again and select **Delete** from the pop-up menu.
- 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**

   - 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.
   - In the **Inventory** pane, select **VMs and Templates**.
   - In the tree view, right-click the vCloud Connector node virtual machine and select **Power > Power Off** from the pop-up menu.
   - 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.
To upgrade vCloud Connector, you need to upgrade your vCloud Connector server and nodes. Note that you can upgrade to vCloud Connector 2.6 from vCloud Connector version 2.5 only. You cannot upgrade from earlier versions to version 2.6.

**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 user interface. Ensure that the **Preserve Favorites Website** data option is deselected in the Delete Browsing History dialog box when you clear the cache.

This chapter includes the following topics:

- “Edit Hardware Settings for vCloud Connector Server and Nodes on vSphere,” on page 85
- “Edit Hardware Settings for vCloud Connector Server and Nodes on vCloud Director,” on page 86
- “Upgrade Server and Nodes,” on page 86
- “Modify Staging Directory Permissions in Upgraded Nodes,” on page 87
- “Update Registration with vSphere Client,” on page 88
- “Verify Your Settings,” on page 88
- “Troubleshooting Upgrade,” on page 89

**Edit Hardware Settings for vCloud Connector Server and Nodes on vSphere**

Before you upgrade your vCloud Connector server and nodes, you must update their virtual hardware settings to match the vCloud Connector 2.6 level. The upgrade process does not update the virtual hardware settings.

Update these settings for the server and for all nodes.

To update hardware settings for servers or nodes installed in vCloud Director, see “Edit Hardware Settings for vCloud Connector Server and Nodes on vCloud Director,” on page 86

**Procedure**

1. Log in to the vSphere Client.
2. Select **Inventory > VMs and Templates**.
3. In the left pane, right-click your vCloud Connector server or node virtual machine and select **Power > Power Off** to power it off.
4. Right-click the server or node and select **Edit Settings**.
5 In the Hardware tab, make the following changes.
   - Select Memory and increase Memory Size to 4 GB.
   - Select CPUs and increase Number of virtual sockets to 4.

6 Click OK.

7 In the left pane, right-click the server or node virtual machine and select Power > Power On to power it on.

What to do next
After you update the hardware settings for your server and nodes, upgrade the server and nodes from the Admin Web console.

Edit Hardware Settings for vCloud Connector Server and Nodes on vCloud Director

Before you upgrade your vCloud Connector server and nodes, you must update their virtual hardware settings to match the vCloud Connector 2.6 level. The upgrade process does not update the virtual hardware settings.

Update these settings for the server and for all nodes.

To update hardware settings for servers or nodes installed in vSphere, see “Edit Hardware Settings for vCloud Connector Server and Nodes on vSphere,” on page 85.

Procedure
1 Log in to the vCloud Director cloud.
2 Click Manage & Monitor and select your organization.
3 Click My Cloud.
4 In the My Cloud panel, select VMs.
5 Select your vCloud Connector server or node virtual machine and click the Power Off icon to power it off.
6 After it is powered off, right-click the node or server and select Properties.
7 Click the Hardware tab and make the following changes.
   - In the CPU section, increase Number of CPUs to 4.
   - In the Memory section, increase Total memory to 4 GB.
8 Click OK.
9 Select your server or node virtual machine and click the Power On icon to power it on.

What to do next
After you update the hardware settings for your server and nodes, upgrade the server and nodes from the Admin Web console.

Upgrade Server and Nodes

To upgrade to vCloud Connector 2.6, upgrade your vCloud Connector 2.5 server and all vCloud Connector 2.5 nodes. You upgrade a vCloud Connector server or node from its Admin Web console.

Note You can upgrade to vCloud Connector 2.6 from vCloud Connector version 2.5 only. You cannot upgrade from earlier versions to version 2.6.
Prerequisites

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

- You have updated the hardware settings of the server or node to the vCloud Connector 2.6 level. See “Edit Hardware Settings for vCloud Connector Server and Nodes on vSphere,” on page 85 and “Edit Hardware Settings for vCloud Connector Server and Nodes on vCloud Director,” on page 86.

- If you use NFS share for the node staging area, modify your settings to use the no_lock option for mounting the NFS share. This is required in vCloud Connector 2.6.

Procedure

1. Go to the vCloud Connector server or node Admin Web console at `https://vCCServerIPaddress:5480` or `https://vCCNodeIPaddress:5480`.

   **Note**: Do not use Firefox as some tabs appear blank on Firefox.

2. Log in as `admin`.

   The default password is `vmware`.

3. Click the Update tab.

4. In the Settings tab, under Update Repository, ensure that Use Default Repository is selected.

5. Click the Status tab, then click Check Updates.

   The available updates appear.

6. Click Install Updates.

7. Accept the EULA.

8. Click OK in the confirmation dialog box and wait for the update process to finish.

9. Click the System tab.

10. Click Reboot.

   You are logged out of the Admin Web console when the system finishes rebooting.

What to do next

After you upgrade the vCloud Connector server and all nodes, do the following.

- “Modify Staging Directory Permissions in Upgraded Nodes,” on page 87.

- “Update Registration with vSphere Client,” on page 88.

Modify Staging Directory Permissions in Upgraded Nodes

After you upgrade a vCloud Connector node to 2.6, change the permissions on the node staging directory. The staging directory must have read, write, and execute permissions for user, group, and other (777). During upgrade, these permissions are incorrectly set to 775, which removes write access to the staging directory for `admin` users. Copy tasks will fail if you do not set the permissions back to 777 on all upgraded nodes.

Procedure

1. Log into the node console as `root`.

2. Type the following command to set the correct permissions.

   `chmod 777 /opt/vmware/hcagent/staging`
What to do next

“Update Registration with vSphere Client,” on page 88.

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 in the Home tab in vSphere Client.

Prerequisites

You have upgraded your vCloud Connector server and nodes to version 2.6.

Procedure

   You can get the IP address of the vCloud Connector server from its console in the vSphere or vCloud Director cloud in which it is installed.
   
   **Note** Do not use Firefox as some tabs appear blank in Firefox.

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 browser cache. Also clear your Internet Explorer cache to ensure new data is shown in the vCloud Connector server and node Admin Web consoles and in the user interface. When you clear the Internet Explorer cache, ensure that the Preserve Favorites Website data option is deselected in the Delete Browsing History dialog box.

Verify Your Settings

After you upgrade vCloud Connector, check your settings.

Log into the server and node Admin Web consoles and check the following.

- Click the System tab and verify that the appliance version is 2.6.
- Verify that your pre-upgrade settings, such as SSL settings, UDT settings, certificates, and hostname have been preserved.
- In the server Admin Web console, click the Nodes tab and check the status of the nodes.
  - Verify that the Local Content Library node appears and that its status is UP.
  - Verify that all nodes registered to the server appear and their status is UP.

Log in to the vSphere Client to which the vCloud Connector UI is registered and do the following.

- Display the Home page of the vSphere Client and verify that the vCloud Connector icon appears under Solutions and Applications.
- Click the vCloud Connector icon and verify that the UI displays all the clouds that were added to it before the upgrade.
- Verify that the Content Library displays any subscriptions that were set up before the upgrade.

**Troubleshooting Upgrade**

You can troubleshoot the upgrade process by checking log files related to upgrade.

The following log files provide upgrade information. Use SSH to log in to the vCloud Connector server or node console to view these files.

- `/opt/vmware/var/log/vami/vami.log`

  After you start the upgrade process for a vCloud Connector server or node by clicking **Install Updates**, you can check the progress of the upgrade or look for errors in the `/opt/vmware/var/log/vami/vami.log` file.

- `/opt/vmware/var/log/postinstall`

  After the upgrade process is complete and the vCloud Connector server or node is rebooted, you can check the `/opt/vmware/var/log/postinstall` file. The following message should appear in the file.

  Finished installing version 2.6.0.0.
Use this information to troubleshoot problems with your vCloud Connector installation.

- **Troubleshooting Storage** on page 91
  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.

- **Troubleshooting Connectivity** on page 92
  You can use cURL to pinpoint connectivity problems among the components of your vCloud Connector installation.

- **Accessing Log Files from the UI** on page 92
  You can download log files for a vCloud Connector server or vCloud Connector node instance from its Admin Web console.

- **Accessing Log Files from the Console** on page 93
  You can access log files for a vCloud Connector server or vCloud Connector node instance from its console.

- **Accessing Log Files for Multitenant Nodes** on page 94
  If you are using a vCloud Connector node that has been deployed as a multitenant node by a public vCloud service provider or private vCloud Director system administrator, you do not have access to the node console or Admin Web console. You can download log files for the node, for your organization only, from your vCloud Connector server Admin Web console.

- **Troubleshooting Log File Size** on page 94
  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.

- **Troubleshooting Upgrade** on page 95
  You can troubleshoot the upgrade process by checking log files related to upgrade.

- **Using Fully Qualified Domain Names (FQDNs)** on page 95
  You can use FQDNs for the vCloud Connector server and vCloud Connector nodes.

**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/organization/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/organization/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 download 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 access log files for your organization only.

**Note** If you are using a multitenant 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 Multitenant 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/hcservor/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 from its console.

Server log files, named hcs.log, are in the /opt/vmware/hcservor/logs directory. Node log files, named hca.log, 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 access log files for your organization only.

**Note** If you are using a multitenant 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 Multitenant 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/hcservor/logs directory.
     ```
     cd /opt/vmware/hcservor/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 a vCloud Connector server) or hca.log file (for a vCloud Connector node).
   Older log files are in a zip file in the same directory.
   For nodes, organization-specific log files are in /opt/vmware/hcagent/logs/Organization/.
   Tomcat log files are named catalina.Date.log.
Accessing Log Files for Multitenant Nodes

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

**Procedure**

2. Log in as **admin**.
   - The default password is **vmware**.
3. Click the **Nodes** tab.
4. Click the gears icon next to the multitenant 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**.
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.

   ```xml
   <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.

Save the file. You do not need to restart.

**Troubleshooting Upgrade**

You can troubleshoot the upgrade process by checking log files related to upgrade.

The following log files provide upgrade information. Use SSH to log in to the vCloud Connector server or node console to view these files.

- `/opt/vmware/var/log/vami/vami.log`

  After you start the upgrade process for a vCloud Connector server or node by clicking **Install Updates**, you can check the progress of the upgrade or look for errors in the `/opt/vmware/var/log/vami/vami.log` file.

- `/opt/vmware/var/log/postinstall`

  After the upgrade process is complete and the vCloud Connector server or node is rebooted, you can check the `/opt/vmware/var/log/postinstall` file. The following message should appear in the file.

  Finished installing version 2.6.0.0.

**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

A
add node to catalog 33, 36
adding vCloud Hybrid Service cloud 58

B
browsers 14

C
certificates 30, 46, 71, 74, 75
checkpoint restart 61
collect information 12
concurrent tasks 46, 77
configure server 28
configure node 44
copy
compatibility 62
large virtual machines or vApps 69
copy options 61
copy protocol 62
create node, vCloud Director 1.5 34
create node, vCloud Director 5.1 37
create server, vCloud Director 5.5 26, 41
create server, vCloud Director 1.5 19
create server, vCloud Director 5.1 22

data encryption 61, 64
data encryption for HTTP(S) 64
data encryption with UDT 65
data transfer protocol
HTTP(S) 64
HTTPS 62, 63
UDT 62, 63
data transfer protocols 63
data transfer flow 79
deployment considerations 16
download 16

F
firewall 20, 23, 26, 35, 38, 42
firewall rules for copy 69
FQDN 95

H
hardware settings, upgrade 85, 86
HTTP copy 64
HTTP(S) protocol 64
HTTP(S) copy 67
HTTPS 62
HTTPS copy 64

I
install node, vCloud Director 5.5 39
install node, vSphere 32
install node, vCloud Director 1.5 32
install node, vCloud Director 5.1 36
install nodes 31
install server, vCloud Director 5.5 24
install Server 17
install Server, vSphere 17
install Server, vCloud Director 1.5 18
install Server, vCloud Director 5.1 21

L
linked mode 18
log files
access 92
size 94
log files, access 93

M
maximum concurrent tasks 46, 77
multiple intermediate SSL certificates 74

N
NAT 20, 23, 26, 35, 38, 42
network settings 29, 45
Network tab, node 45
Network tab, server 29
Node, Service Provider 57
node storage 76
node storage, vSphere 76
node storage, vCloud Director 77
Node tab 46
nodes 7
Nodes tab 31

O
overview 5, 7, 11
P
password 30, 46
path optimization 61, 62
planning installation 8
ports 14
production 71
proxy server
  HTTP(S) copy 67
  UDT copy 66
proxy settings 29, 45

R
reboot, node 44
reboot, server 28
register UI, vSphere Client 50
register nodes with clouds 43
register nodes with server 49
register UI 50
requirements 14

S
server 7
Server tab 30
Service Provider Node 57
service provider deployment 53
Service Provider node 57
setting copy options 61
SSL 64
SSL certificates 30, 46, 71, 74, 75
staging directory permissions 87
System tab, node 44
System tab, server 28

T
time zone settings 28, 44
troubleshooting, log 60, 94
troubleshooting, connectivity 92
troubleshooting, log 92
troubleshooting, storage 91
troubleshooting, log file size 94
troubleshooting, overview 91
trusted keystore 75

U
UDP 62
UDT 62
UDT properties 66
UDT protocol 63
UDT copy 66
UDT encryption 64, 65
udt_pkt_size 66
udt_snd_buf 66
UDT_rcv_buf 66
UI 7, 50
uninstall 81
uninstall, nodes 82
uninstall, server 81
update registration, upgrade 88
update policy 29, 46
Update tab, node 46
Update tab, server 29
upgrade
  hardware settings 85
  resetting permissions 87
  troubleshooting 89, 95
  update registration 88
upgrade, hardware settings, hardware
  settings 86
upload node to catalog 33, 36
upload server to catalog 19, 22, 25, 40

V
vCloud Hybrid Service 58, 59
view data transfer protocol 63