Installing and Configuring vCloud Connector

vCloud Connector 2.7.0

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

EN-001609-01

vmware
You can find the most up-to-date technical documentation on the VMware Web site at:
http://www.vmware.com/support/
The VMware Web site also provides the latest product updates.
If you have comments about this documentation, submit your feedback to:
docfeedback@vmware.com
Contents

Installing and Configuring vCloud Connector   5

1 vCloud Connector Overview   7
   About vCloud Connector   7
   Planning Your vCloud Connector Installation   9

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   25
   Install vCloud Connector Nodes   28
   Register vCloud Connector Nodes with Clouds   36
   Configure vCloud Connector Nodes   37
   Register vCloud Connector Nodes with vCloud Connector Server   42
   Register the vCloud Connector User Interface   43

3 Deploying Multitenant Nodes as a vCloud Service Provider   45

4 Using Service Provider Multitenant Nodes   49
   Use vCloud Service Provider Nodes   49
   Use vCloud Air vCloud Connector Nodes   50
   Accessing Log Files for Multitenant Nodes   50

5 Selecting Copy Options   51
   About vCloud Connector Copy   51
   Compatibility with Earlier Versions of vCloud Connector   52
   Data Transfer Protocols for Copy   52
   Data Encryption   54
   Set UDT Properties   56
   Using Proxy Servers   56
   Firewall Rules for Copying Between Private and Public Clouds   59
   Copying Large Virtual Machines or vApps   59

6 Preparing vCloud Connector for Production Use   61
   Add Valid SSL Certificates   61
   Upload Certificates from the Command Line   64
   Add CA Root Certificate to Trusted Keystore   65
   Configure vCloud Connector Node Allocated Storage   66
7 Cross-Cloud Data Transfer and Network Connectivity 69

8 Uninstalling vCloud Connector 71
   Uninstall a vCloud Connector Server 71
   Uninstall vCloud Connector Nodes 72

9 Upgrading vCloud Connector 75
   Upgrade Server and Nodes 75
   Update Registration with vSphere Client 76
   Verify Your Settings 76
   Troubleshooting Upgrade 77

10 Troubleshooting vCloud Connector 79
   Troubleshooting Storage 79
   Troubleshooting Connectivity 80
   Accessing Log Files from the User Interface 80
   Accessing Log Files from the Console 81
   Accessing Log Files for Multitenant Nodes 82
   Troubleshooting Log File Size 82
   Troubleshooting Upgrade 83
   Using Fully Qualified Domain Names (FQDNs) 83

Index 85
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 user interface.

**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 9

About vCloud Connector

vCloud Connector provides a single user interface for overseeing multiple private and public clouds and for transferring content from one cloud to another.

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 VMware vCloud Air™.

vCloud Connector Components

vCloud Connector consists of three distinct components: the vCloud Connector user interface, the vCloud Connector server, and vCloud Connector nodes.
vCloud Connector User Interface

The vCloud Connector user interface appears as a plug-in in the vSphere Client to which it is registered. The vCloud Connector icon appears in the vSphere Client Home page, under Solutions and Applications.

NOTE The vCloud Connector user interface is not available for the vSphere Web Client.

vCloud Connector Server

The vCloud Connector server is a virtual appliance that coordinates the activity of vCloud Connector, controls vCloud Connector nodes, and creates the vCloud Connector user interface. 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 or private vCloud Director-based clouds, the service provider or cloud administrator can install a vCloud Connector node as a multitenant node for multiple customers to use so that each customer does not have to install their own node in their organization.

In vCloud Air, a vCloud Connector node is installed by VMware by default. You do not need to install a node in vCloud Air.
Planning Your vCloud Connector Installation

Before you install vCloud Connector, decide the following.

- Where you want to install the vCloud Connector server
  You can install the server in vSphere or vCloud Director.

- Which clouds you want to be able to add to the vCloud Connector user interface. You must install a vCloud Connector node in each cloud that you want to add.
  To add vCloud Director clouds, you can either install a node in your organization or use the node that the cloud administrator or service provider may have installed as a multitenant node.

  **Note** For information on deploying a multitenant node as a service provider or cloud administrator, see Chapter 3, “Deploying Multitenant Nodes as a vCloud Service Provider,” on page 45.

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

- Which vSphere Client you want to use for the vCloud Connector user interface
  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. See “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**

You install a vCloud Connector node in each cloud that you want to connect. To connect a public vCloud Director-based 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 Air cloud instance, you use the vCloud Connector 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 multiple, private vSphere and vCloud Director instances
- Connect one or more private vSphere or vCloud Director instances with a public vCloud Director-based cloud
Connect one or more private vSphere or vCloud Director instances with vCloud Air

Procedure

1. **Collect Necessary Information** on page 12
   
   Use 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 25
   
   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 28
   
   You can install vCloud Connector nodes in vSphere or vCloud Director clouds.

8. **Register vCloud Connector Nodes with Clouds** on page 36
   
   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 37
   
   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 42
    
    After you install a vCloud Connector server and nodes, you use the server Admin Web console to register the nodes with the server. The registration allows the server to manage the nodes.

11. **Register the vCloud Connector User Interface** on page 43
    
    You register the vCloud Connector user interface with vSphere Client.

Collect Necessary Information

Use 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></td>
<td></td>
</tr>
<tr>
<td>• VMware® vCenter Server™ administrator account</td>
<td>User name, password, and URL or IP address</td>
<td>Installing vCloud Connector server</td>
</tr>
<tr>
<td>• VMware vCloud Director® account with at least organization administrator status</td>
<td></td>
<td></td>
</tr>
<tr>
<td>vCenter Server administrator account for each vSphere cloud</td>
<td>User name, password, and URL or IP address</td>
<td>Installing vCloud Connector node</td>
</tr>
<tr>
<td>vCloud Director account with at least organization administrator status for each vCloud Director cloud</td>
<td>User name, password, and URL or IP address</td>
<td>Installing vCloud Connector node</td>
</tr>
<tr>
<td>vCenter Server administrator account or any account that has Extension privileges for the vCenter Server in which you want to use the vCloud Connector user interface</td>
<td>User name, password, and FQDN or IP address</td>
<td>Registering the vCloud Connector user interface</td>
</tr>
</tbody>
</table>

### Proxy Servers

You need the following proxy information.

### Table 2-2. Proxy Information

<table>
<thead>
<tr>
<th>Information Needed</th>
<th>Condition</th>
</tr>
</thead>
<tbody>
<tr>
<td>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>
</tr>
<tr>
<td>User name and password, if the proxy server requires authentication. See “Network Tab (Server)”, on page 26 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>

**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.
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 69.

Displaying the vCloud Connector User Interface

To set up the vCloud Connector user interface in vSphere Client, you need the following information.

Table 2-4. vCloud Connector user interface in vSphere

<table>
<thead>
<tr>
<th>Information Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IP address or fully qualified domain name (FQDN) 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 user interface 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>
<tbody>
<tr>
<td>vSphere</td>
<td>4.0 update 3, 4.1, 5.0, 5.1, 5.5.x</td>
<td>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.</td>
</tr>
<tr>
<td>vCloud Director</td>
<td>5.1, 5.5, 5.6.2, 5.6.3, 5.8, 5.9</td>
<td>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.</td>
</tr>
<tr>
<td>vShield Manager</td>
<td>5.1.2, 5.1.3, 5.5, 5.5.2</td>
<td>Required for the Stretch Deploy feature (Datacenter Extension) only.</td>
</tr>
<tr>
<td>vSphere Client</td>
<td>4.0 update 3, 4.1, 5.0, 5.1, 5.5.x</td>
<td>Required for the vCloud Connector UI. The vCloud Connector UI is registered as a plug-in in vSphere Client.</td>
</tr>
</tbody>
</table>

**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 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.

### 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 69.

**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 endpoint.

- 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 45.

**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**

A My VMware account.

**Procedure**

2. Click **Download Now**.
3 Scroll down to the **Product Downloads** section and download both the vCCServer and vCCNode zip files.
   a Click **Download**.
   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 Save 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 an administrator account for the vSphere instance in which you want to deploy the vCloud Connector server. You 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 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 25.

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 user interface with a vSphere Client Associated with a Linked Mode vCenter Server Configuration

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

When you register the user interface, specify the IP address or URL of any of the vCenter Server instances. The user interface 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 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 19
   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 19
   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 20
   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 20.

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.
Double-click your virtual datacenter.

Click the **Org VDC Networks** tab.

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

Click the **NAT** tab.

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

The Add Destination NAT Rule dialog box appears.

Specify the external IP address.

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.

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

Click **OK**.

Click **Add SNAT**.

The Add Source NAT Rule dialog box appears.

Select the network on which to apply the rule.

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

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

Click **OK**.

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

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.

Select the **Enabled** check-box.

Give the rule a name.

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

Type the destination IP address and port.

The destination IP address is the external IP address.

Select the protocol.

Select **Allow**.

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.
Add the vCloud Connector Server to a vCloud Director 5.5 Catalog as a vApp Template on page 22

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.
   - Under Source, select Local file, click Browse, and select the vCloud Connector server OVF file that you downloaded.
   - 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 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 powered on and you have its IP address. 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**.
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.

For more information about network paths in data transfers, see Chapter 7, “Cross-Cloud Data Transfer and Network Connectivity,” on page 69.

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 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>Setting Description</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>To check for updates automatically</td>
<td>Select <strong>Automatic check for updates</strong>, then set the frequency for the update check.</td>
</tr>
<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 user interface.

General

The **General Settings** section allows you to change the administrator password for the vCloud Connector server, set log levels, and download log files.

<table>
<thead>
<tr>
<th>Setting Description</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change admin user password</td>
<td>Specify a new administrator password for the vCloud Connector server, then click <strong>Confirm new password</strong>. You should change the default password.</td>
</tr>
<tr>
<td>Log levels</td>
<td>Set the log level for the vCloud Connector server log file, then click <strong>Change log level</strong>.</td>
</tr>
<tr>
<td>Download logs</td>
<td>Click to download a zip file of vCloud Connector server log files.</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Setting Description</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable SSL/Enable SSL</td>
<td>Select <strong>Enable SSL</strong> 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.</td>
</tr>
<tr>
<td>Key Information</td>
<td>Displays information about the default key provided.</td>
</tr>
<tr>
<td>Certificate Information</td>
<td>Displays information about the self-signed certificate that is provided with the vCloud Connector server.</td>
</tr>
<tr>
<td>Generate New Key</td>
<td>If you need to generate a new private key to obtain a valid certificate from your Certificate Authority, specify the required information and click <strong>Generate Key</strong>. In the <strong>Common Name</strong> field, specify the IP address or fully-qualified domain name of the vCloud Connector server. For example, <strong>10.10.10.10</strong> or <strong>myServer.mycompany.com</strong>.</td>
</tr>
<tr>
<td>Generate and download CSR</td>
<td>Click to create a Certificate Signing Request and save it to your computer. Use the saved hcservcer.csr file to get a certificate from your Certificate Authority.</td>
</tr>
<tr>
<td>Upload a new X.509 SSL Certificate</td>
<td>When you have your certificate, use the <strong>Browse</strong> button to locate it, then click <strong>Upload</strong>.</td>
</tr>
</tbody>
</table>
For more information on installing valid certificates, see “Add Valid SSL Certificates,” on page 61.

vSphere Client Tab

The vSphere Client tab is used to register the vCloud Connector user interface. For more information, see “Register the vCloud Connector User Interface,” on page 43.

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. During the initial installation process, you use this tab after you install nodes.

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 2-8. Options

<table>
<thead>
<tr>
<th>Task</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>To register a node with the server</td>
<td>Click Register Node. See “Register vCloud Connector Nodes with vCloud Connector Server,” on page 42.</td>
</tr>
<tr>
<td>To edit a node's registration</td>
<td>Click the gears icon next to the node and select Edit. See “Register vCloud Connector Nodes with vCloud Connector Server,” on page 42.</td>
</tr>
<tr>
<td>To unregister a node from the server</td>
<td>Click the gears icon next to the node and select Unregister.</td>
</tr>
<tr>
<td>To download node log files</td>
<td>Click the gears icon next to the node and select Download Logs.</td>
</tr>
<tr>
<td>To specify Stretch Deploy settings</td>
<td>Click the gears icon next to the node and select Stretch Deploy Settings. See Using Stretch Deploy in Using vCloud Connector.</td>
</tr>
<tr>
<td>To unregister Stretch Deploy settings</td>
<td>Click the gears icon next to the node and select Unregister Stretch Deploy Settings. See Using Stretch Deploy in Using vCloud Connector.</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 a public or private vCloud Director cloud, you can either install a node in your organization in the cloud or use a multitenant node installed by the service provider or cloud administrator.

To use a multitenant node, you need to get the node URL from the service provider or system administrator. See “Use vCloud Service Provider Nodes,” on page 49 for more information.

**Note** For information on deploying a multitenant node as a service provider or cloud administrator, see Chapter 3, “Deploying Multitenant Nodes as a vCloud Service Provider,” on page 45.

To connect a vCloud Air cloud instance, you use the node installed by VMware in vCloud Air. You do not need to install your own node in vCloud Air.

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 have administrator-level privileges for the vSphere instance. You 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 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 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 45 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 30
   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 31
   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 32
   If you select a NAT-based network connection when you deploy your vCloud Connector node, you need to set up NAT mapping and firewall rules.

---

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

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

**Prerequisites**

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

**Procedure**

1. Log in to the vCloud Director Web console using a supported browser.
2. Click **Catalogs**.
   - If you log in as System Administrator, select your organization first, then click the **Catalogs** tab.
3. Select the catalog to which you want to upload the vCloud Connector node, then click the **vApp Templates** tab.
4. Click the **Upload** icon.
5. In the Upload OVF package as a vApp Template popup, click **Browse** and select the node OVF file that you downloaded.
6. Specify a name and, optionally, a description, for the vApp template.
7. Select the virtual datacenter, catalog, and storage profile for the template.
8. Click **Upload**.

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

**NOTE** It may take several seconds after the upload itself has finished for the process to be finalized.
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 32.
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.
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 45 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 34
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 34
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 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 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 appear blank 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 65 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 is powered on and you have its IP address. You have the information you collected in “Collect Necessary Information,” on page 12.

**Procedure**

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

2 If you receive a certificate warning, accept the certificate.
3 Log in as admin.
   The default password is vmware.
   Check the Web console title to make sure you are configuring the vCloud Connector node.
4 Use the information you collected to complete general configuration as needed.
5 When you finish the general configuration tasks, log out of the vCloud Connector node Admin Web console.

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

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

Time Zone
The Time Zone tab allows you to set your local time zone. Select a time zone, then click Save Settings.
The virtual hardware clock is always maintained in UTC, which the virtual appliance converts to local time. Correct local time is important for the update repository and VMware Update Manager.

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

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

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

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

   NOTE If you set a static IP address you must make sure that there are values for all the displayed fields. In vCloud Director installations, you must set Preferred and Alternate DNS servers manually. Talk to your service provider or network administrator for the appropriate addresses.

For more information about network paths in data transfers, see Chapter 7, “Cross-Cloud Data Transfer and Network Connectivity,” on page 69.
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>Setting</th>
<th>Option</th>
</tr>
</thead>
<tbody>
<tr>
<td>To check for updates automatically</td>
<td>Select <strong>Automatic check for updates</strong>, then set the frequency for the update check.</td>
</tr>
<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**.
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 the cloud it manages.

Cloud

In the Cloud Registration section, you register the vCloud Connector node with the cloud it manages.

**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 system administrator of the cloud.

<table>
<thead>
<tr>
<th><strong>Cloud Type</strong></th>
<th>The type of cloud.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cloud URL</strong></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>- <a href="https://CloudIPaddress">https://CloudIPaddress</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://CloudFQDN">https://CloudFQDN</a></td>
</tr>
<tr>
<td></td>
<td>For example: <a href="https://cloud1.company.com">https://cloud1.company.com</a></td>
</tr>
<tr>
<td><strong>Ignore SSL Cert</strong></td>
<td>Select this option if the cloud does not have a valid SSL certificate or if you do not want to use the certificate.</td>
</tr>
<tr>
<td></td>
<td><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 65 for information on importing the certificate.</td>
</tr>
<tr>
<td><strong>Use Proxy</strong></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 Network - Proxy tab.</td>
</tr>
</tbody>
</table>

General

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

<table>
<thead>
<tr>
<th><strong>Change admin user password</strong></th>
<th>Specify a new administrator password for the vCloud Connector node, then click Confirm new password. Changing the default password is recommended.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Log levels</strong></td>
<td>Set the log level for vCloud Connector node log file, then click Change log level.</td>
</tr>
<tr>
<td><strong>Download logs</strong></td>
<td>Click to download a zip file of vCloud Connector node log files. <strong>Note</strong>: If you are using a multitenant node deployed on a public or private vCloud Director cloud by a service provider or system administrator, or a node deployed by VMware on vCloud Air, you do not have access to the node. You can download your log files from the vCloud Connector server Admin Web console instead.</td>
</tr>
<tr>
<td><strong>Concurrent Tasks</strong></td>
<td>Specify the maximum number of concurrent tasks that are allowed for the vCloud Connector node, then click Change Maximum Concurrent Tasks. The default is 10. <strong>Note</strong>: 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 for Nodes,” on page 68 and “Configure vCloud Connector Node Allocated Storage,” on page 66 for more information.</td>
</tr>
</tbody>
</table>
UDT is a data transfer protocol that can be used instead of HTTP(S) to copy data. **UDT Status** displays whether UDT is currently enabled or disabled for the node. Select **Enable UDT** or **Disable UDT** to enable or disable UDT.

When UDT is disabled, HTTP(S) is used to copy data.

**Note** You must select the **Enable UDT** 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 51 for more information.

### 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 57 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 54 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**.

**Generate and download CSR**

Click to create a Certificate Signing Request and save it to your computer. Use the savedhcagent.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 64.
For more information on installing valid certificates, see “Add Valid SSL Certificates,” on page 61.

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 registration allows the server to manage the nodes.

The nodes can be installed on vSphere, private vCloud Director clouds, public vClouds, or vCloud Air.

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.

See also Chapter 4, “Using Service Provider Multitenant Nodes,” on page 49.

Prerequisites

To register a multitenant node deployed on a public or private vCloud Director cloud, obtain the node URL from the service provider or cloud administrator. To register a node deployed in vCloud Air by VMware, obtain the node URL from VMware.

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>Display Name</td>
<td>A name for the cloud. The cloud will appear by this name in the vCloud Connector user interface.</td>
</tr>
<tr>
<td>Node URL</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>
<tr>
<td>Public</td>
<td>Select this option if the cloud is a public cloud outside the firewall where your vCloud Connector server is installed.</td>
</tr>
</tbody>
</table>
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 node deployed on a public cloud by a service provider, 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. You must use a valid organization name. vCloud Connector validates the name that you provide with the cloud.
| **Note** If you selected vSphere in the Cloud Type option, this field is disabled.
| **Note** If you are registering a node deployed on a public cloud by a service provider, specify the name of your organization in the public cloud. If you are registering a node deployed by VMware on vCloud Air, specify the name of your virtual data center in vCloud Air. See Chapter 4, “Using Service Provider Multitenant Nodes,” on page 49 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 User Interface**

You register the vCloud Connector user interface with vSphere Client.

**Register the vCloud Connector User Interface in vSphere Client**

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

Use a vCenter server administrator role or any user role that includes Extension privileges to register the user interface.

You can register the vCloud Connector user interface 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, or have unregistered and are registering again, clear your Internet Explorer cache before you register. 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**

- The IP address or fully qualified domain name of the vCenter Server to which the vSphere Client is pointed.
- 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**.
   The default password is **vmware**.
4. Click the **Server** tab, and click the **vSphere Client** tab.
5. The vCloud Connector server URL 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

Figure 3-1. Deploying Multitenant Nodes

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 endpoint.
- 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 51.
- 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.


   **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 61 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 65 for information.

5. Increase the node staging area. See “Configure vCloud Connector Node Allocated Storage,” on page 66 for information.

   **Note** If you use NFS share to increase the staging area, use the noLock 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 console.
   b Change to root user.
      
      ```
      su root
      ```
      
      The default password is vmware.
   c Edit the /etc/hosts file and add the following line as the first entry.
      ```
      multitenantNodeInternalIP multitenantNodeFQDN
      ```
   d Exit the console.

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 42.

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 81 and “Accessing Log Files from the User Interface,” on page 80 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 50 for more information.

### Upgrading a Multitenant Node

To upgrade a multitenant node, follow the process described in Chapter 9, “Upgrading vCloud Connector,” on page 75. 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 user interface.
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 user interface. 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 vCloud Service Provider Nodes,” on page 49
- “Use vCloud Air vCloud Connector Nodes,” on page 50
- “Accessing Log Files for Multitenant Nodes,” on page 50

Use vCloud 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 Air cloud instance to your vCloud Connector installation, see “Use vCloud Air vCloud Connector Nodes,” on page 50.

### 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.
   
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.
   
Use vCloud Air vCloud Connector Nodes

You can connect a vCloud Air cloud instance to vCloud Connector by using the vCloud Connector node deployed by VMware in vCloud Air.

You register the node with your on-premise vCloud Connector server using the node URL obtained from VMware and your vCloud Air credentials.

See the Installing VMware vCloud Connector for VMware vCloud Air document for information about connecting your on-premise environment with vCloud Air using vCloud Connector.

Accessing Log Files for Multitenant Nodes

If you are using a multitenant node deployed by a public vCloud service provider or private vCloud Director system administrator, or a node deployed by VMware on vCloud Air, you do not have access to the node console or Admin Web console. You can download node log files from your vCloud Connector server Admin Web console instead.

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.
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 51
- “Compatibility with Earlier Versions of vCloud Connector,” on page 52
- “Data Transfer Protocols for Copy,” on page 52
- “Data Encryption,” on page 54
- “Set UDT Properties,” on page 56
- “Using Proxy Servers,” on page 56
- “Firewall Rules for Copying Between Private and Public Clouds,” on page 59
- “Copying Large Virtual Machines or vApps,” on page 59

About vCloud Connector Copy

vCloud Connector uses 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 66 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 54.
  
  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 54.
  
  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 57 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 54 and “Enabling Data Encryption for UDT Data Transfer Protocol,” on page 55.
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 54 and “Enabling Data Encryption for HTTP(S) Transfer Protocol,” on page 54.
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, the buffer size for UDT in source and destination clouds, and the minimum and maximum bandwidth for UDT transfer.

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.

Similarly, in high latency and packet loss scenarios, configuring the minimum bandwidth to slightly less than the actual bandwidth available improves copy performance.

You can set the following properties.

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
<th>Default Value</th>
<th>Recommended Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>udt_pkt_size</td>
<td>Packet size of UDT packets</td>
<td>1048576 KB</td>
<td>For low bandwidth networks: 1024-1048576 (1KB to 1MB)</td>
</tr>
<tr>
<td>udt_snd_buf_size</td>
<td>Buffer size of UDT at the source</td>
<td>10485760 KB</td>
<td>Approximately 10 times udt_pkt_size</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The value must be greater than udt_pkt_size</td>
</tr>
<tr>
<td>udt_rcv_buf_size</td>
<td>Buffer size of UDT at the destination</td>
<td>10485760 KB</td>
<td>Approximately 10 times udt_pkt_size</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>The value must be greater than udt_pkt_size</td>
</tr>
<tr>
<td>udt_min_bw</td>
<td>Sets the minimum bandwidth for UDT transfer, for optimal throughput</td>
<td>1 Mbps</td>
<td>Slightly less than the actual bandwidth available. If the value is too high, performance is degraded.</td>
</tr>
<tr>
<td>udt_max_bw</td>
<td>Sets the maximum bandwidth for UDT transfer</td>
<td>0 Mbps</td>
<td>In most cases you do not need to set the maximum bandwidth.</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](image)

Procedure

1. Enable UDT on the source and destination nodes.
   See “Select UDT Protocol for Data Transfer,” on page 53.

2. Enable encryption for UDT transfer on the destination node.
   See “Enabling Data Encryption for UDT Data Transfer Protocol,” on page 55.

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, 10.10.10.10.</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.

**Figure 5.2. Using a Proxy Server with HTTP(S)**

**Procedure**

1. Enable HTTP(S) on the source and destination nodes.
   See “Select HTTP(S) Protocol for Data Transfer,” on page 54.

2. Enable encryption for HTTPS transfer on the destination node.
   See “Enabling Data Encryption for HTTP(S) Transfer Protocol,” on page 54.

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, <strong>10.10.10.10</strong>.</td>
</tr>
<tr>
<td>Proxy Port</td>
<td>The proxy port.</td>
</tr>
</tbody>
</table>
| Proxy Username    | (Optional) The user name for the proxy server, if the proxy server requires authentication.  
|                   | **Note**: Specify a user name that contains lower-case, alpha-numeric characters only and does not exceed 50 characters. Do not use email addresses or domain names (for example, user@company.com or xyz\user) or names that contain a period (for example, firstname.lastname) as special characters are not supported for this field. |
| Proxy Password    | (Optional) The password for the proxy server, if the proxy server requires authentication. |
Click **Save Settings**.

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>Source</th>
<th>Port</th>
<th>Protocol</th>
<th>Destination</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Node</td>
<td>HTTPS any</td>
<td>TCP</td>
<td>Public Node</td>
<td>HTTPS 443</td>
</tr>
<tr>
<td>Private Node</td>
<td>HTTP any</td>
<td>TCP</td>
<td>Public Node</td>
<td>HTTP 80</td>
</tr>
<tr>
<td>Private Node</td>
<td>UDP any</td>
<td>UDP</td>
<td>Public Node</td>
<td>UDP 8190</td>
</tr>
<tr>
<td>Server</td>
<td>HTTPS any</td>
<td>TCP</td>
<td>Public Node</td>
<td>HTTPS 443</td>
</tr>
<tr>
<td>Server</td>
<td>HTTP any</td>
<td>TCP</td>
<td>Public Node</td>
<td>HTTP 80</td>
</tr>
<tr>
<td>Server</td>
<td>HTTPS any</td>
<td>TCP</td>
<td>Public Cloud</td>
<td>HTTPS 443</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**

If you plan to copy large virtual machines, vApps, or templates, configure your source or destination environments with the settings listed here.

Note that copying large workloads with vCloud Connector can take several hours, depending on the size of the object you are copying and on network conditions.

**Increase Transfer Session Timeout for Destination vCloud Director Clouds**

If you are copying to a vCloud Director cloud, increase the transfer session timeout in vCloud Director to avoid a timeout error during upload.

1. Log in to the vCloud Director instance as a system administrator.
2. Click the **System** tab, then the **Administration** tab.
3. In the **Administration** pane, click **General**.
4. Under **Timeouts**, increase the value of **Transfer session timeout**.

**Increase Transfer Spooling Area for vCloud Director Clouds**

If you are copying to or from a vCloud Director cloud, increase the transfer server storage, also known as the transfer spooling area, in vCloud Director. See the [vCloud Director documentation](https://example.com) for more information.
Increase Source and Destination Node Staging Area

While vCloud Connector copy, which is a streaming operation, does not write files to the staging area of the source or destination nodes during copy, in some cases staging area storage is required. For example, if export from the cloud to the source node is faster than the transfer from the source node to the destination node, data is buffered in the staging area.

Increasing the staging area storage in the source and destination nodes to the size of the object you are copying is recommended. See “Configure vCloud Connector Node Allocated Storage,” on page 66 for information.
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 61
- “Upload Certificates from the Command Line,” on page 64
- “Add CA Root Certificate to Trusted Keystore,” on page 65
- “Configure vCloud Connector Node Allocated Storage,” on page 66
- “Increase Maximum Concurrent Tasks for Nodes,” on page 68

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 65.

vCloud Connector supports wildcard certificates.

**Procedure**

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

2. Log in as `admin`.

   The default password is `vmware`. 
3 For vCloud Connector server, click the **Server** tab, then click the **SSL** tab. For vCloud Connector node, click the **Node** tab, then click the **SSL** tab.

4 Create a new private key if your Certificate Authority requires you to do so. You can create a 2048-bit key either through the Admin Web console or the command line interface.

**NOTE** For a wildcard certificate with a Common Name containing a special character such as *, generate the key from the command line as the Common Name field in the Admin Web console does not support special characters.

To generate a 2048-bit key through the Admin Web console, 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.  You can only 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 using the command line interface, complete these steps.

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

   The default password is **vmware**.

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

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

   For the node, change to this directory.

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

c Delete the existing key.

   For the server, use this command.

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

   For the node, use this command.

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

d Generate the new 2048-bit key.
For the server, use this command.
/usr/java/default/bin/keytool -genkey -keyalg RSA -keysize 2048 -alias hcserver -validity 1095 -keystore tcserver.jks -storepass changeme -keypass changeme

For the node, use this command.
/usr/java/default/bin/keytool -genkey -keyalg RSA -keysize 2048 -alias hcagent -validity 1095 -keystore tcserver.jks -storepass changeme -keypass changeme

e Log out of the console.

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

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

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

   **NOTE** If you are obtaining certificates from a Windows Server 2008 Certificate Authority, select the 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.

   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 42.

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 65 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.

```
/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 42.

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 root. 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.

    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.

    cd /usr/java/default/jre/lib/security

5 Import the root certificate.

    /usr/java/default/bin/keytool -import -trustcrls -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.
Right-click the vCloud Connector node virtual appliance and select **Open Console**.

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

The default password is **vmware**.

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.

    ```
    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 for Nodes

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 involve both a source cloud and a destination cloud, you should increase the storage for both.

**Note** The Copy command has a different limit for concurrent copy tasks. See "How Objects are Copied" in Using vCloud Connector for more information.

**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 66.
vCloud Connector manages the transfer of content using a separate component, the vCloud Connector node. This flow affects the way a request moves through the system and how network connectivity must be set up.

**Data Flow in Transfer**

The following figure shows the path a vCloud Connector request takes in transferring data from a vSphere to a vCloud Director (VCD) cloud.

**Note** This figure depicts default settings. Port 443 is used when SSL is enabled and port 80 is used when SSL is disabled. By default, SSL is disabled for the vCloud Connector server and enabled for vCloud Connector nodes.

Enabling or disabling SSL on the vCloud Connector server affects communication from the vCloud Connector UI to the server. Enabling or disabling SSL on vCloud Connector nodes affects communication from the server to the nodes and communication between nodes.

**Figure 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 71
- “Uninstall vCloud Connector Nodes,” on page 72

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.
To remove the server from a vCloud Director cloud, complete these steps.

a Log in to the vCloud Director cloud.

b Click the My Cloud tab.

c In the My Cloud panel, select vApps.

d Find your vCloud Connector server vApp in the Name column, right-click it, and select Stop from the pop-up menu.

e When the Status column displays Stopped for the vCloud Connector server vApp, right-click it again and select Delete from the pop-up menu.

f Click Yes to confirm.

The vCloud Connector server is now deleted. You cannot access vCloud Connector from the vSphere Client.

Uninstall vCloud Connector Nodes

You can uninstall a vCloud Connector node from a cloud if you no longer want to transfer content to and from that cloud. You must also uninstall vCloud Connector nodes when you uninstall vCloud Connector.

Procedure

1 Go to the vCloud Connector server Admin Web console at https://vccServerIPaddress:5480.
   You can get the IP address of the vCloud Connector server from its console in the vSphere Client or vCloud Director cloud in which it is installed.

2 Log in as admin.
   If you did not change the password, use vmware, the default password.

3 Click the Nodes tab.

4 Click the gears icon next to the vCloud Connector node to delete, then select Unregister from the pop-up menu.
   The node is now unregistered from the server.

5 Repeat Step 4 for all the nodes you want to delete. If you are uninstalling vCloud Connector, delete all the nodes that are registered with the server.

6 Log in to the cloud in which the vCloud Connector node is installed.

7 If the node is installed on a vSphere cloud, delete it from the cloud.
   a In the Inventory pane, select VMs and Templates.
   b In the tree view, right-click the vCloud Connector node virtual machine and select Power > Power Off from the pop-up menu.
   c When the vCloud Connector node virtual machine is powered off, right-click it again and select Delete from Disk from the pop-up menu.
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.
Upgrading vCloud Connector

To upgrade vCloud Connector, you need to upgrade the vCloud Connector server and nodes, and update the server’s registration with the vSphere Client.

Upgrade is supported for the following versions.

- From versions 2.6 or 2.6.1 to version 2.7
- From version 2.7 to version 2.7.1

**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:

- “Upgrade Server and Nodes,” on page 75
- “Update Registration with vSphere Client,” on page 76
- “Verify Your Settings,” on page 76
- “Troubleshooting Upgrade,” on page 77

## Upgrade Server and Nodes

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

**Prerequisites**

- You have the IP address of the vCloud Connector server or node. You can get the IP address from its console.
- If you use NFS share for the node staging area, modify your settings to use the `nolock` option for mounting the NFS share.

**Procedure**

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

   **Note** Use Internet Explorer or Chrome. 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, then the **Settings** tab.

4 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 and 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, “**Update Registration with vSphere Client**,” on page 76.

---

**Update Registration with vSphere Client**

After you upgrade the vCloud Connector server and nodes, you must update the server’s registration with the vSphere Client, otherwise vCloud Connector does not appear in the vSphere Client.

#### Prerequisites

You have upgraded your vCloud Connector server and nodes.

#### Procedure

1 Go to the vCloud Connector server Admin Web console at https://vCCServerIPaddress:5480.
   - You can get the IP address of the server from its console.

   **Note**: Use Internet Explorer or Chrome. 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 the upgraded version.
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 user interface 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 user interface displays all the clouds that were added to it before the upgrade.
- Verify that the Content Library displays all 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 n.
Troubleshooting vCloud Connector

Use this information to troubleshoot problems with your vCloud Connector installation.

- **Troubleshooting Storage** on page 79
  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 80
  You can use cURL to pinpoint connectivity problems among the components of your vCloud Connector installation.

- **Accessing Log Files from the User Interface** on page 80
  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 81
  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 82
  If you are using a multitenant node deployed by a public vCloud service provider or private vCloud Director system administrator, or a node deployed by VMware on vCloud Air, you do not have access to the node console or Admin Web console. You can download node log files from your vCloud Connector server Admin Web console instead.

- **Troubleshooting Log File Size** on page 82
  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 83
  You can troubleshoot the upgrade process by checking log files related to upgrade.

- **Using Fully Qualified Domain Names (FQDNs)** on page 83
  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 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.
   
   ```bash
   curl -k -v https://vcd-host/api/versions
   ```
3. Test the connection between the vCloud Connector server and a vCenter Server.
   
   ```bash
   curl -k -v https://vc-host/mob
   ```
4. Test the connection between the vCloud Connector server and a vCloud Connector node.
   
   ```bash
   curl -k -v https://node-host/agent/api/v2/org/org/version
   ```
5. Log in to the vCloud Connector node located in the vSphere internal cloud to test the node connections used in the copy path.
6. Test the connection between the vCloud Connector node and the vCenter Server.
   
   ```bash
   curl -k -v https://vc-host/mob
   ```
7. Test the connection between the vCloud Connector node and the ESX host.
   
   ```bash
   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.
   
   ```bash
   curl -k -v https://node-host/agent/api/v2/org/org/version
   ```
9. Log in to the vCloud Director vCC node.
10. Test the connection between the vCloud Director vCC node and the vCloud Director cloud.
    
    ```bash
    curl -k -v https://vcd-host/api/versions
    ```

Accessing Log Files from the User Interface

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 50.
**Procedure**

1. Go to the vCloud Connector server or vCloud Connector node Admin Web console at https://Server_or_Node_IPaddress:5480.
2. Log in as `admin`. The default password is `vmware`.
3. Download the log files.
   - In the server Admin Web console, click the **Server** tab, then click the **General** tab and click **Download logs**.
   - In the node Admin Web console, click the **Node** tab, then click the **General** tab and click **Download logs**.
4. Save the zip file.
5. Extract files from the zip file.
   - The node log file is named `hca.log` and is in the `opt/vmware/hcagent/logs` directory. The server log file is named `hcs.log` and is in the `opt/vmware/hcserver/logs` directory.
   - Older log files are in a zip file in the same directory.
   - Tomcat log files are named `catalina.Date.log`.

**Accessing Log Files from the Console**

You can access log files for a vCloud Connector server or vCloud Connector node instance from its console.

Server log files, named `hcs.log`, are in the `/opt/vmware/hcserver/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 50.

**Procedure**

1. In your vSphere Client or vCloud Director cloud, open the server or node console and log in as `admin`. The default password is `vmware`.
2. Change directory.
   - In the server console, go to the `/opt/vmware/hcserver/logs` directory.
     ```bash
cd /opt/vmware/hcserver/logs
```
   - In the node console, go to the `/opt/vmware/hcagent/logs` directory.
     ```bash
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 multitenant node deployed by a public vCloud service provider or private vCloud Director system administrator, or a node deployed by VMware on vCloud Air, you do not have access to the node console or Admin Web console. You can download node log files from your vCloud Connector server Admin Web console instead.

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.
   
   `<rollingPolicy class="ch.qos.logback.core.rolling.FixedWindowRollingPolicy">
   <fileNamePattern>/opt/vmware/hcserver or hcagent/logs/hcs.%i.log.zip or hca.%i.log.zip</fileNamePattern>
   <minIndex>1</minIndex>
   <maxIndex>9</maxIndex>
   </rollingPolicy>
   
   `<triggeringPolicy class="ch.qos.logback.core.rolling.SizeBasedTriggeringPolicy">
   <maxFileSize>10MB</maxFileSize>
   </triggeringPolicy>

To modify the number of files to retain, change rollingPolicy/maxIndex to the desired number.
To modify the size of log files, change `triggeringPolicy/maxFileSize` to the desired size.

**NOTE** This is the size of a single file, so the total log size could be as large as this value times the `maxNumber` value. Archived log files are zipped, however, so the total log size is usually much smaller.

5. Save the file. You do not need to restart.

**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 n.

**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 30

B
browsers 14

C
certificates 27, 40, 61, 64, 65
checkpoint restart 51
collect information 12
concurrent tasks 40, 68
configure server 25
configure node 37
copy
  compatibility 52
  large virtual machines or vApps 59
copy options 51
copy protocol 52
create node, vCloud Director 5.1 31
create server, vCloud Director 5.5 23, 34
create server, vCloud Director 5.1 19

D
data encryption 51, 54
data encryption for HTTP(S) 54
data encryption with UDT 55
data transfer protocol
HTTP(S) 54
HTTPS 52, 53
UDT 52, 53
data transfer protocols 53
data transfer flow 69
deployment considerations 16
download server and node 16

F
firewall 20, 23, 32, 35
firewall rules for copy 59
FQDN 83

H
HTTP copy 54
HTTP(S) protocol 54
HTTP(S) copy 58
HTTPS 52

I
HTTPS copy 54
install node, vCloud Director 5.5 33
install node, vSphere 29
install node, vCloud Director 5.1 29
install nodes 28
install server, vCloud Director 5.5 21
install Server 17
install Server, vSphere 17
install Server, vCloud Director 5.1 18

L
linked mode 18
log files
  access 80
  size 82
log files, access 81

M
maximum concurrent tasks 40, 68
multiple intermediate SSL certificates 64

N
NAT 20, 23, 32, 35
network settings 26, 38
Network tab, node 38
Network tab, server 26
Node, Service Provider 49
node storage 66
node storage, vSphere 66
node storage, vCloud Director 67
Node tab 40
nodes 7
Nodes tab 28

O
overview 5, 7, 11

P
password 27, 40
path optimization 51, 52
planning installation 9
ports 14
production 61
proxy server
  HTTP(S) copy 58
  UDT copy 57
proxy settings 26, 38

R
reboot, node 38
reboot, server 25
register UI 43
register UI, vSphere Client 43
register nodes with clouds 36
register nodes with server 42
requirements 14

S
server 7
Server tab 27
Service Provider Node 49
service provider deployment 45
Service Provider node 49
setting copy options 51
SSL 54
SSL certificates 27, 40, 61, 64, 65
System tab, node 38
System tab, server 25

T
time zone settings 25, 38
troubleshooting, log 50, 82
troubleshooting, connectivity 80
troubleshooting, log 80
troubleshooting, storage 79
troubleshooting, log file size 82
troubleshooting, overview 79
trustrd keystore 65

U
UDP 52
UDT 52
UDT properties 56
UDT protocol 53
UDT copy 57
UDT encryption 54, 55
udt_pkt_size 56
udt_rcv_buf 56
udt_snd_buf 56
UI 7, 43
uninstall 71
uninstall, nodes 72
uninstall, server 71
update registration, upgrade 76
update policy 26, 39

Update tab, server 26
Update tab, node 39
upgrade
  troubleshooting 77, 83
  update registration 76
upload node to catalog 30
upload server to catalog 19, 22, 34

V
vCloud Air 50
view data transfer protocol 53