Installation and Configuration

vCloud Connector 1.5.0

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

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

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

Contents

Installation and Configuration for vCloud Connector

Installation and Configuration for vCloud Connector provides a brief overview of vCloud ® Connector™ 1.5.0 and vcloud.vmware.com. It also gives detailed information on installing and configuring vCloud Connector Server and vCloud Connector Nodes and setting up the vCloud Connector UI .

Intended Audience

This information is intended for anyone who wants to set up vCloud Connector (vCC). You should be familiar with vSphere Client, the vCloud Director Web console, and deploying virtual appliances.

vCloud Connector Overview 1

This section provides an overview of vCloud Connector and the vcloud.vmware.com website.

It includes information on the functionality of vCloud Connector and the components that make it up. It also describes vcloud.vmware.com, a website that extends the functionality of vCloud Connector to the browser.

■ vCloud Connector on page 7

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

■ The vcloud.vmware.com Website on page 8

The website vcloud.vmware.com allows you to access the vCloud Connector UI through your browser.

■ Planning Your vCloud Connector Installation on page 9

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

vCloud Connector

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

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

vCloud Connector Components

vCloud Connector consists of three distinct components:the vCloud Connector UI, the vCloud Connector Server, and vCloud Connector Nodes.

Figure 1-1. vCloud Connector Components
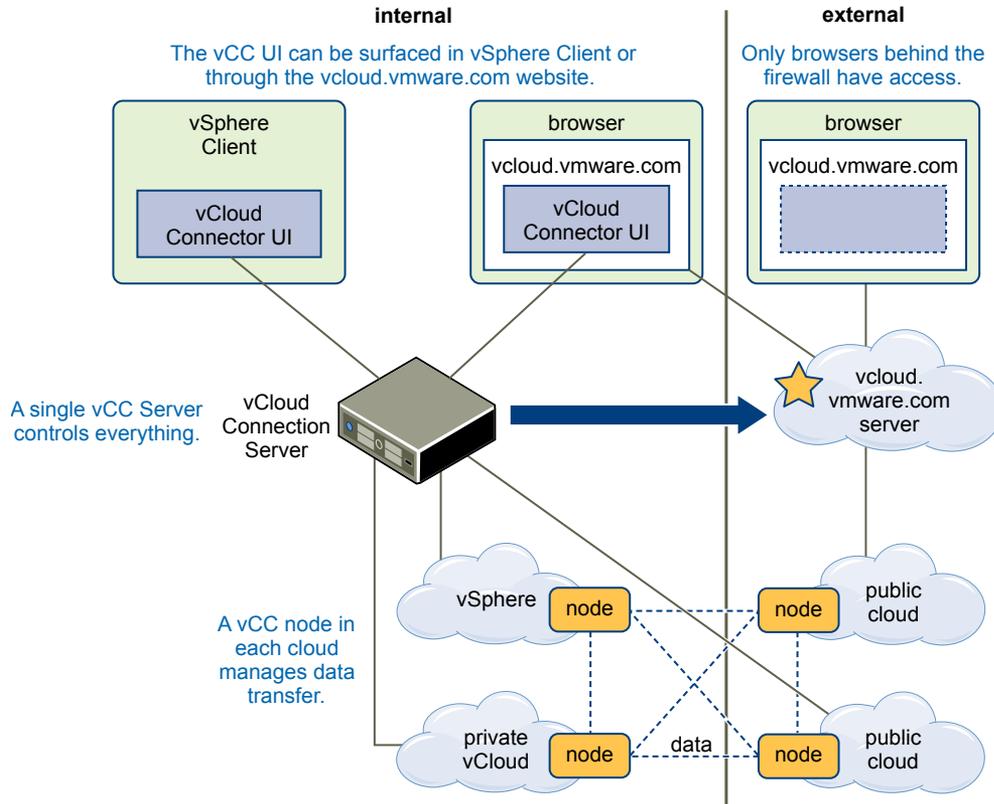
vCloud Connector UI

vCloud Connector UI is the user interface that vCloud Connector Server produces. It can be surfaced in vSphere Client or at vcloud.vmware.com. If you decide to display your UI via vcloud.vmware.com, and your vCC Server is behind a firewall, only browsers also behind the firewall can see the UI. You decide where to display the UI during the configuration process.

vCloud Connector Server

vCloud Connnector Server is a virtual appliance that coordinates the activity of vCloud Connector, controls vCloud Connector Nodes, and produces the vCloud Connector UI. Only one vCloud Connector Server is needed.

vCloud Connector Nodes

vCloud Connector Nodes are virtual appliances that handle transferring content from one cloud to another. Transfers between clouds that are interrupted, for example because of network problems, can be resumed at the point that they were interrupted. A vCloud Connector Node must be installed in every vSphere or vCloud cloud that vCloud Connector oversees.

The vcloud.vmware.com Website

The website vcloud.vmware.com allows you to access the vCloud Connector UI through your browser.

The website is designed to help you make the move to a hybrid cloud environment. You can view your vCloud Connector through it and you can share access to your clouds with others. The website also connects you to a range of public cloud service providers offering evaluation cloud offers and a community of other vCloud Connector users.

Planning Your vCloud Connector Installation

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

You need to decide:

- Where you want to install the vCloud Connector Server

- Which clouds you want to be able to add to the vCloud Connector UI. For each addition you wish to make, you must install a copy of vCloud Connector Node in that cloud.

- Where you want to access the vCloud Connector UI, in the vSphere Client, on vcloud.vmware.com, or both.

You also need to collect specific information to use during the installation and configuration process. What you need to know depends on your specific installation decisions. A detailed description of the information you should collect is covered in "Collect Necessary Information," on page 12.

Installing vCloud Connector

2

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

Figure 2-1. vCloud Connector Installation and Configuration Workflow
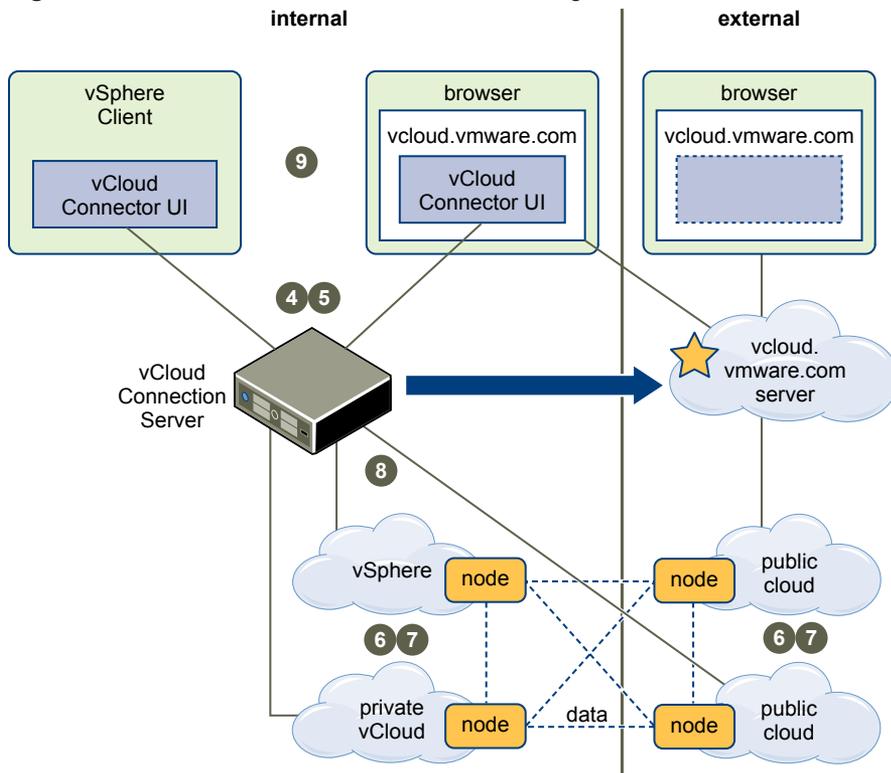
Procedure

1 Collect Necessary Information on page 12

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

2 Check Requirements on page 14

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

3   Download the vCloud Connector Virtual Appliances on page 15

vCloud Connector Server and vCloud Connector Nodes are packaged as virtual appliances. You download the virtual appliances from the vcloud.vmware.com website or the vCloud Connector 1.5 Download page.

4   Install vCloud Connector Server on page 15

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

5   Configure vCloud Connector Server on page 22

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

6   Install vCloud Connector Nodes on page 24

You can install vCloud Connector Nodes in vSphere, or in vCloud Director 1.0, 1.0.1, or 1.5 clouds.

7   Configure vCloud Connector Nodes on page 30

You use the vCC Node admin Web console for each of your nodes 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.

8   Register vCloud Connector Nodes with vCloud Connector Server on page 32

You use the vCC Server admin Web console to register vCC Nodes (installed on vSphere or private / public vClouds) with vCC Server. This allows the vCC Server to manage the Nodes.

9   Register the vCloud Connector UI on page 33

You can register the vCloud Connector UI to appear in your vSphere Client, vcloud.vmware.com, or both.

10   Prepare vCloud Connector for Production Use on page 34

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

Collect Necessary Information

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

Accounts

You need the following accounts:

Table 2-1. Account Information

Account Type	Information Needed	Used For
A vmware.com store account. Store accounts are free from vmware.com.	Username and password	Accessing vcloud.vmware.com
One of the following: ■ vCenter Server administrative account ■ vCloud Director account with at least Org Administrator status	Username, password and URL or IP address for the appropriate entity	Installing vCC Server

Table 2-1. Account Information (Continued)

Account Type	Information Needed	Used For
vCenter Server administrative account for each vSphere cloud	Username, password and URL or IP address	Installing vCC Node
vCloud Director with at least Org Administrator status for each vCD cloud	Username, password and URL or IP address	Installing vCC Node

Proxy Servers

You need the following proxy information:

Table 2-2. Proxy Information

Install Type	Information Needed	Condition
vCC Server	host:port NOTE username/password not supported	If the Server needs a proxy to be able to access systems beyond the firewall in the location in which it is installed.
vCC Node - per Node	host:port NOTE username/password not supported	If the vCC Node needs a proxy to be able to access systems beyond the firewall in the location in which it is installed.

Network

If you are using a static IP (not using DHCP) for vCC Server or vCC Node, you need the following information for each instance.

Table 2-3. Network Information

Network Information
An available static IP address
The netmask for that address
The IP address of the gateway
The IP address of a primary and secondary DNS server
A hostname (optional)

For more information on network paths in data transfers, see Chapter 3, "Cross-Cloud Data Transfer and Network Connectivity," on page 39.

Displaying the vCloud Connector UI

If you want to set up the vCC UI to display in a vSphere Client, you need to know:

Table 2-4. vCC UI in vSphere

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

If you want to display the vCC UI at vcloud.vmware.com, you need to know:

Table 2-5. vCC UI in vcloud.vmware.com

vCC UI in vcloud.vmware.com
The vmware.com account username and password with which you want to access vCC UI via vcloud.vmware.com.
The IP adresss or fully qualified domain name of the vCC Server. This information is assigned when the Server is first deployed.

Check Requirements

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

To successfully deploy and configure vCloud Connector Server and Nodes, make sure you have the following:

■ vSphere 4.x or 5.0

or

■ vCloud Director 1.0, 1.0.1, or 1.5

NOTE If you are deploying on vSphere, you also need:

■ A Microsoft Windows desktop with vSphere Client installed.

■ Microsoft Internet Explorer 7 or later.

This is a requirement for vSphere Client. The browser must be set to accept third-party cookies.

If you are deploying on vCloud Director, you also need:

■ A supported browser

　■ Internet Explorer 7+

　■ Firefox 3+

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

If you have users who will be accessing vCD 1.0 virtual machine consoles through the vCC UI running as a plug-in in a vSphere Client 4.x, , you need to make sure you are running an update release of vSphere Client which supports launching consoles. The following releases of vSphere Client work:

■ 4.0U3

■ 4.1U2

NOTE This is the only case that requires a vSphere Client update release. You must use a supported browser.

Download the vCloud Connector Virtual Appliances

vCloud Connector Server and vCloud Connector Nodes are packaged as virtual appliances. You download the virtual appliances from the vcloud.vmware.com website or the vCloud Connector 1.5 Download page.

Prerequisites

You have collected the information specified in "Collect Necessary Information," on page 12.

Procedure

1 Point your browser to vcloud.vmware.com.

    You can also get the virtual appliances from the vCloud Connector Download page.

2 Log in using your vmware.com store account.

    If you do not have a vmware.com store account, register at www.vmware.com. The account is free.

3 Click **vCloud Connector** in the left navigation bar.

4 Click **Download**.

5 Read and accept the EULA.

6 Click **zip** for the vCC Server virtual appliance and download it to your desktop.

7 Click **zip** for the vCC Node virtual appliance and download it to your desktop.

8 In separate directories, unzip the vCC Server and the vCC Node virtual appliance zip files.

Install vCloud Connector Server

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

Only one vCC 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 vCloud Connector Server in vSphere 4.0, 4.1, or 5.0.

Prerequisites

You must have an administrative account on the vSphere in which you deploy the vCloud Connector Server. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 15.

Procedure

1 Log in to vSphere Client.

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

3 Click **Browse** to navigate to the OVF directory of the Server zip file.

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 22

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

7   Using the vSphere Client, power on the vCC Server.

8   Find the vCC Server's IP address (not the Host) in the **Summary** tab for the Server in the vSphere Client interface. Make a note of the IP address. You will need it later in the process.

Install vCloud Connector Server in vCloud Director 1.0 and 1.0.1

You can install vCC Server in vCloud Director 1.0 or 1.0.1.

NOTE   If you install vCC Server in a public cloud, you can only connect to public clouds in your vCC UI.

Prerequisites

You must have at least Organization Administrator access in the vCloud Director on which you install the vCC Server.

Procedure

1   Add the vCloud Connector Server to a vCloud Director 1.0 or 1.0.1 Catalog as a vApp Template on page 16

Before you can deploy vCC Server in a vCloud Director 1.0 or 1.0.1 cloud, you must upload the virtual appliance to the 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 on page 17

After the vCC Server software is added to the vCloud Director 1.0 or 1.0.1 cloud as a template, it can be used to create a running instance in that cloud.

3   Set Up NAT Mapping - vCloud Connector Server and vCloud Director 1.0 and 1.0.1 on page 18

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

Add the vCloud Connector Server to a vCloud Director 1.0 or 1.0.1 Catalog as a vApp Template

Before you can deploy vCC Server in a vCloud Director 1.0 or 1.0.1 cloud, you must upload the virtual appliance to the 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 access on the vCloud Director on which you install the vCC Node. You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 15

Procedure

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

2   Click **Manage Catalogs**.

You must upload the vCC Server software to a Catalog as a template before you can deploy it.

3   In the appropriate Catalog, click the **Upload** icon.

4   In the Upload OVF package as a vApp Template pop-up window, click **Browse** and navigate to the OVF directory of the Server zip file you downloaded.

5   Give the vApp template a name in the text box.

6   Click **Upload**.

The template is uploaded. You can monitor the status of the upload in the Transfer Progress pop-up window.

NOTE It might take several seconds after the upload is finished before the upload process finalizes in the cloud.

Create the vCloud Connector Server from the Template

After the vCC Server software is added to the vCloud Director 1.0 or 1.0.1 cloud as a template, it can be used to create a running instance in that cloud.

Prerequisites

You must have Organization Administrator access on the vCloud Director on which you install the vCC Server.

Procedure

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

The first screen of the **Add to My Cloud** popup appears.

2   Give the vCC Server vApp an easily identifiable name and make normal decisions on lease times., and click **Next**.

3   Read and accept the EULA and click **Next**.

4   On the Configure Virtual Machines page, select the appropriate vDC for the Server instance from the drop-down menu.

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

Unless all of your vCC Nodes and the server are behind the same firewall and you do not plan to use vcloud.vmware.com to access the vCC UI, you must select a network that is configured to access the Internet. Ask your service provider or network administrator for more information.

NOTE   If your provider uses NAT, you will need to set up NAT mapping after your Server is deployed. See "Set Up NAT Mapping - vCloud Connector Server and vCloud Director 1.0 and 1.0.1," on page 18

---

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 Admin for more information

7   On the Configure Networking page, leave both check boxes unchecked and click **Next**.

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

9   Click the **My Cloud** tab.

You see the vApp being created.

10   In the **My Cloud** tab of your vCloud Director 1.1 or 1.0.1 Web console, right-click the console icon of the vCC Server and select **Start**.

11   When the vCC Server on vCloud Director 1.0 or 1.0.1 is in running state, right-click the console icon again and select **Open**.

12   Click the **Virtual Machine** tab and note the IP address of the vCC Server.

You need the IP address later in the registration process.

Set Up NAT Mapping - vCloud Connector Server and vCloud Director 1.0 and 1.0.1

If you select a NAT-based network connection when you deploy your vCC 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 vCC operation or to forward all ports and then set up a firewall rule to filter all but the following required ports:

- Port 8443: For communication between vCC Server and Node and between Nodes.
- Port 5480: For communication with the Web admin interface for the appliance, for example during the registration process.

Prerequisites

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

Procedure

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

2   Find the network you are using in the Networks list and right-click.

3   Select **Configure Services...** from the Network Menu.

    The Configure Services popup appears.

4   Click the **NAT Mapping** tab and click **Add** at the bottom of the popup to create the NAT rule.

    The Add NAT Rule popup appears.

5   Select one of the External IPs available from the drop-down list.

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

6   To NAT all ports, enter an asterisk (*) for the first port entry.

    To NAT only the two required ports, add a rule for each port.

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

8   Click **OK** and click **OK** again.

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

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

    Create two rules, one for each necessary port.

    The Add Firewall Rule popup appears.

11 Give the rule a name and select the **Incoming** radio button.

12 Type the source IP address and the source port.

    For incoming traffic, the source is the external network. This is the address you selected in Step 5

13 Type the destination IP and port.

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

14 Select the **Allow** action.

15 Select the **Enabled** check box.

16 Click **OK** and **OK** to create the rule.

Install vCloud Connector Server in vCloud Director 1.5

You can install vCloud Connector Server in vCloud Director 1.5.

NOTE   If you install vCC Server in a public cloud, you can only connect to public clouds in your vCC UI.

Prerequisites

You must have at least Organization Administrator access in the vCloud Director on which you install the vCC Server.

Procedure

1   Add the vCloud Connector Server to a vCloud Director 1.5 Catalog as a vApp Template on page 19

   Before you can deploy vCC Server in a vCloud Director 1.5 cloud, you must upload the virtual appliance to the 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 on page 20

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

3   Set Up NAT Mapping - vCloud Connector Server and vCloud Director 1.5 on page 21

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

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

Before you can deploy vCC Server in a vCloud Director 1.5 cloud, you must upload the virtual appliance to the 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 access on the vCloud Director on which you install the vCC Server.You must have the unzipped version of the template you downloaded in "Download the vCloud Connector Virtual Appliances," on page 15

Procedure

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

2   Click **Catalogs**.

3   In the appropriate Catalog, click **vApp Templates**.

   You must upload the vCC Server software to a Catalog as a template before you can deploy it.

4   Click the **Upload** icon.

5   In the Upload OVF package as a vApp Template pop-up window, click **Browse** and navigate to the OVF directory of the Server zip file you downloaded.

6   Give the vApp template a name in the text box.

7   (Optional) Select the vDC and Catalog for this template, using the drop-down lists.

8   Click **Upload**.

The template is uploaded. You can monitor the status of the upload in the **Transfer Progress** pop-up window.

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

Create the vCloud Connector Server from the Template

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

Prerequisites

You must have Organization Administrator access on the vCloud Director on which you install the vCC Server.

Procedure

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

    The first screen of the Add to My Cloud popup appears.

2   Give the vCC Server vApp an easily identifiable name, make normal decisions on lease times, and click **Next**.

3   Read and accept the EULA and click **Next**.

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

    Unless all your vCC Nodes and the Server are behind the same firewall and you do not plan to use vcloud.vmware.com to access the vCC UI, select a network that is configured to access the Internet. Ask your Service Provider or Network Admin for more information.

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

    Unless all of your vCC Nodes and the server are behind the same firewall and you do not plan to use vcloud.vmware.com to access the vCC UI, you must select a network that is configured to access the Internet. Ask your service provider or network administrator for more information.

    NOTE   If your provider uses NAT, you will need to set up NAT mapping after your Server is deployed. See "Set Up NAT Mapping - vCloud Connector Server and vCloud Director 1.0 and 1.0.1," on page 18

6   On the Configure Networking page, leave both check boxes unselected, and click **Next**.

7   On the Ready to Complete page, review the settings and click **Finish**.

8   Select the **My Cloud** tab.

    You see the vApp being created in the **vApp** section.

9   Click **VMs** and right-click your vCC Server to select **Properties**.

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

11 Select **Enable guest customization**.

12 Click **Okay**.

13 On the **My Cloud** tab of your vCloud Director 1.5 Web console, select **vApps**, then right-click the console icon of the vCC Server and select **Start**.

14 When the vCC Server on vCloud Director 1.5 is in running state, click **VMs** in the left selection bar and make a note of the IP address.

    You need the IP address later in the registration process.

Set Up NAT Mapping - vCloud Connector Server and vCloud Director 1.5

If you select a NAT-based network connection when you deploy your vCC 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 vCC operation or to forward all ports and then set up a firewall rule to filter all but the following required ports:

- Port 8443: For communication between vCC Server and Node and between Nodes.

- Port 5480: For communication with the Web admin interface for the appliance, for example during the registration process.

Prerequisites

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

Procedure

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

2   Find the network you are using in the Networks list and right-click.

3   Select **Configure Services...** from the Network Menu.

    The Configure Services popup appears.

4   Click the **NAT Mapping** tab and click **Add** at the bottom of the popup to create the NAT rule.

    The Add NAT Rule popup appears.

5   Select one of the External IP addresses from the drop-down list.

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

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

    If you wish to NAT only the two required ports, create two rules, one for each port.

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

8   Click **OK** and click **OK** again.

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

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

    Create two rules, one for each necessary port.

    The Add Firewall Rule popup appears.

11 Give the rule a name and select the **Incoming** radio button.

12 Type the source IP address and the source port.

    For incoming traffic, the source is the external network. This is the address you selected in Step 5

13 Type the destination IP address and port.

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

14 Select the **Allow** action.

15 Select the **Enabled** check box.

16 Click **OK** and **OK** to create the rule.

Configure vCloud Connector Server

You use the vCC 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.

The vCC Server admin Web console interface is divided into five tabs, with the first three tabs, **System**, **Network**, and **Update**, and part of the fourth, **Server**, being used for general configuration.

Prerequisites

The vCC Server instance is running and you have the IP address for it that you wrote down when you installed it. You also have the information you gathered in "Collect Necessary Information," on page 12

Procedure

1 Open the vCC Server admin Web console interfaceby pointing your browser to https://*<IP address>*:5480.

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

3 Log into the vCC Server admin Web console as admin.using the default username `admin` and the default password `vmware`.

   The default password is vmware. Check the Web console title to confirm that you are configuring the vCC Server.

4 Use the information you collected in "Collect Necessary Information," on page 12 to complete general configuration.

5 When you have finished with general configuration, keep the vCC Server admin Web console page open to the **Server** tab in your browser.

System Tab - Server

The **System** tab provides general information on the virtual appliance, allows you to configure times zones, and gives you buttons to shutdown and reboot the appliance.

Information

The main **Information** section provides general information on the virtual appliance, such as the version number and the hostname. It also contains the **Reboot** and **Shutdown** buttons.

Time Zone

The **Time Zone** section allows you to set your local time zone. Click **Time Zone** to see a drop-down menu displaying time zones of the world. Select a time zone and click **Save Settings**.

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

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.

Network Tab - Server

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

Status

The **Network Status** section 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** section allows you to 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 of the displayed fields. In vCD installations, you must set Preferred and Alternate DNS servers manually. Talk to your Service Provider or Network Admin for the appropriate addresses. You recorded the information that you need for these settings in "Collect Necessary Information," on page 12

For more information about network paths in data transfers, see Chapter 3, "Cross-Cloud Data Transfer and Network Connectivity," on page 39

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

Proxy

The **Proxy Settings** section allows you to set up any necessary proxy settings, including address and port. Set this if the appliance must use a proxy to reach systems beyond the firewall at the installation location.

NOTE   Proxies that require a username/password are not supported.

You recorded the information that you need for these settings in "Collect Necessary Information," on page 12

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

Update Tab - Server

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

Status

The **Status** section allows you to view information about your virtual appliance or to check for and install updates. Click **Check Updates** to check for updates from the update repository, shown in the **Available Updates** pane. Click **Install Updates** to install the updates.

Settings

The **Update Settings** section allows you to determine when you want to check for updates. You should leave the **Use Default Repository** button selected. Save any changes you make by clicking **Save Settings**.

Server Tab

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

General

The **General Settings** section allows you to change the administrative password for the Server.

NOTE   You should change the password for the Server from the default.

You can also set log levels and download logs using this section. Use the drop down menu to select the log level from TRACE, DEBUG, INFO, WARN, or ERROR and then click **Change Log Level**to save your change. To download a zip of all log files, click **Download logs**.

SSL

The **Manage SSL Certificates** section allows you to manage your certificates. vCloud Connector Node includes a self-signed certificate. Before going into production, replace that with a valid certificate.

In this section, you can see the certificate currently assigned to your vCloud Connector Node.

Click **Generate and Download CSR** to create a Certificate Signing Request. For more information on installing a valid certificate, see "Add Valid SSL Certificates," on page 35

If you prefer to use your own self-signed certificate, click **Generate and Install.**

Install vCloud Connector Nodes

You can install vCloud Connector Nodes in vSphere, or in vCloud Director 1.0, 1.0.1, or 1.5 clouds.

You must install a Node in every cloud you want to connect and oversee using vCloud Connector.

Install vCloud Connector Node in vSphere

You can install vCC Node in vSphere 4.0, 4.1, or 5.0.

Prerequisites

You must have vSphere administrative access on the vSphere in which you install vCC Node.

Procedure

1   Log in to vSphere Client.

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

3   Click **Browse** and navigate to the OVF directory of the Node zip file you downloaded to your desktop in "Download the vCloud Connector Virtual Appliances," on page 15.

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

Install vCloud Connector Node in vCloud Director 1.0 and 1.0.1

You install a copy of vCC Node in each vCloud Director 1.0 or 1.0.1 cloud you want to connect to and use with vCC.

Prerequisites

You must have at least Organization Administrator access on the vCloud Director on which you install the vCC Node.

Procedure

1   Add the vCloud Connector Node to a vCloud Director 1.0 or 1.0.1 Catalog as a vApp Template on page 25

Before you can deploy vCC Node in a vCloud Director 1.0 or 1.0.1 cloud, you must upload the virtual appliance to the 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 on page 26

After the vCC Node software is added to the vCloud Director 1.0 or 1.0.1 cloud as a template, you can use it to create a running instance on that cloud.

3   Set Up NAT Mapping - vCloud Connector Node and vCloud Director 1.0 and 1.0.1 on page 26

If you select a NAT-based network connection when you deploy your vCC Node, you need to set up NAT mapping and, potentially, firewall rules.

Add the vCloud Connector Node to a vCloud Director 1.0 or 1.0.1 Catalog as a vApp Template

Before you can deploy vCC Node in a vCloud Director 1.0 or 1.0.1 cloud, you must upload the virtual appliance to the 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 Organization Administrator access on the vCloud Director on which you install the vCC Node.

Procedure

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

2   Click **Manage Catalogs**.

You must upload the vCC Node software to a Catalog as a template before you can deploy it.

3   In the appropriate Catalog, click the **Upload** icon.

4   In the Upload OVF package as a vApp Template popup, 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 15.

5   Give the vApp template a name in the text box.

6   Click **Upload**.

The template is uploaded. You can see the status of the upload in the Transfer Progress pop-up window.

NOTE   It might take several seconds after the upload itself has finished for the upload process to finalize in the cloud.

Create the vCloud Connector Node from the Template

After the vCC Node software is added to the vCloud Director 1.0 or 1.0.1 cloud as a template, you can use it to create a running instance on that cloud.

Prerequisites

You must have Organization Administrator access on the vCloud Director on which you install the vCC Node.

Procedure

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

The first screen of the **Add to My Cloud** popup appears.

2   Give the vCC Node vApp an easily identifiable name and make normal decisions on lease times,clicking **Next** when you are done.

3   Read and accept the EULA and click **Next**.

4   On the Configure Virtual Machines page, use the drop down menu to select the appropriate vDC for the Node instance.

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

Unless all the nodes controlled by your vCC 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 Admin 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 - vCloud Connector Node and vCloud Director 1.0 and 1.0.1," on page 26

6   Select an appropriate IP Assignment from the drop-down menu. If there is a static IP pool, that is probably a reasonable choice. Ask your Service Provider or Network Admin for more information. Click **Next** to continue.

7   On the Configure Networking page, leave both check boxes unselected and click **Next**.

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

9   Click the **My Cloud** tab.

You see the vApp being created.

Set Up NAT Mapping - vCloud Connector Node and vCloud Director 1.0 and 1.0.1

If you select a NAT-based network connection when you deploy your vCC Node, you need to set up NAT mapping and, potentially, firewall rules.

There are multiple approaches to managing this issue. Decide whether you wish to use NAT to forward only the ports necessary for vCC operation or to forward all ports and then set up a firewall rule to filter all but the following required ports:

■   Port 8443: For communication between vCC Server and Node and between Nodes.

■   Port 5480: For communication with the Web admin interface for the appliance, for example during the registration process.

Prerequisites

Your appliance is deployed and you are logged into the vCD Web console.

Procedure

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

2   Find the network you are using in the Networks list and right-click.

3   Select **Configure Services...** from the Network Menu.

The Configure Services popup appears.

4   Click the **NAT Mapping** tab and click **Add** at the bottom of the popup to create the NAT rule.

The Add NAT Rule popup appears.

5   Select one of the External IPs available from the drop-down list.

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

6   To NAT all ports, enter an asterisk (*) for the first port entry.

To NAT only the two required ports, add a rule for each port.

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

8   Click **OK** and click **OK** again.

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

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

Create two rules, one for each necessary port.

The Add Firewall Rule popup appears.

11   Give the rule a name and select the **Incoming** radio button.

12   Type the source IP address and the source port.

For incoming traffic, the source is the external network. This is the address you selected in Step 5

13   Type the destination IP and port.

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

14   Select the **Allow** action.

15   Select the **Enabled** check box.

16   Click **OK** and **OK** to create the rule.

Install vCloud Connector Node in vCloud Director 1.5

You install a copy of vCC Node in each vCloud Director 1.5 cloud you want to connect to and use with vCC.

Prerequisites

You must have at least Organization Administrator access on the vCloud Director on which you install the vCC Node.

Procedure

1   Add the vCloud Connector Node to a vCloud Director 1.5 Catalog as a vApp Template on page 28

Before you can deploy vCC Node in a vCloud Director 1.5 cloud, you must upload the virtual appliance to the 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 on page 28

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

3

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

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

Before you can deploy vCC Node in a vCloud Director 1.5 cloud, you must upload the virtual appliance to the 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 Organization Administrator access on the vCloud Director on which you install the vCC Node.

Procedure

1 Log into vCloud Director Web console using a supported browser.

2 Click**Catalogs**.

3 In the appropriate Catalog, click **vApp Templates**

You must upload the vCC Node software into a Catalog as a template before you can deploy it.

4 Click the Upload icon.

5 In the Upload OVF package as a vApp Template popup, click **Browse** and navigate to OVF directory of the Node zip file you downloaded to your desktop in "Download the vCloud Connector Virtual Appliances," on page 15.

6 Give the vApp template a name in the text box.

7 If you wish, select the vDC and Catalog for this template, using the drop down boxes.

8 Click **Upload**.

9 The **Transfer Progress** popup lets you monitor the status of the upload.

The template is uploaded.

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

Create the vCloud Connector Node from the Template

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

Prerequisites

You have Organization Administrator access on the vCloud Director on which you install the vCC Node.

Procedure

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

The first screen of the Add to My Cloud popup appears.

2 Give the vCC Node vApp an easily identifiable name and make normal decisions on lease times, clicking **Next** when you are done.

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

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

Unless all the nodes controlled by your vCC 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 Admin for more information.

5   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 Admin 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 - vCloud Connector Node and vCloud Director 1.5," on page 29

6   On the Configure Networking page, leave both check boxes unchecked and click **Next**.

7   On the Ready to Complete page, review the settings and click **Finish**.

8   Click the **My Cloud** tab.

You see the vApp being created in the vApp section.

9   Select **VMs**, right-click your vCC Node, and select **Properties**.

10 On the Virtual Machine Properties page, select the **Guest OS Customization** tab.

11 Check **Enable guest customization**.

12 Click **Okay**.

Set Up NAT Mapping - vCloud Connector Node and vCloud Director 1.5

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

There are multiple approaches to managing this issue. Decide whether you wish to use NAT to forward only the ports necessary for vCC operation or to forward all ports and then set up a firewall rule to filter all but the following required ports:

- Port 8443: For communication between vCC Server and Node and between Nodes.

- Port 5480: For communication with the Web admin interface for the appliance, for example during the registration process.

Prerequisites

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

Procedure

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

2   Find the network you are using in the Networks list and right-click.

3   Select **Configure Services...** from the Network Menu.

The Configure Services popup appears.

4   Click the **NAT Mapping** tab and click **Add** at the bottom of the popup to create the NAT rule.

The Add NAT Rule popup appears.

5   Select one of the External IP addresses from the drop-down list.

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

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

If you wish to NAT only the two required ports, create two rules, one for each port.

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

8   Click **OK** and click **OK** again.

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

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

    Create two rules, one for each necessary port.

    The Add Firewall Rule popup appears.

11   Give the rule a name and select the **Incoming** radio button.

12   Type the source IP address and the source port.

    For incoming traffic, the source is the external network. This is the address you selected in Step 5

13   Type the destination IP address and port.

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

14   Select the **Allow** action.

15   Select the **Enabled** check box.

16   Click **OK** and **OK** to create the rule.

Configure vCloud Connector Nodes

You use the vCC Node admin Web console for each of your nodes 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.

The vCC Node admin Web console interface is divided into four tabs: System, Network, Update, and Node.

Prerequisites

The vCC Node instance is running and you have the IP address for it that you wrote down when you installed it. You have the information you collected in "Collect Necessary Information," on page 12

Procedure

1   Open the vCC Node Admin Web console interface by pointing your browser to https://*<IP address>*:5480.

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

3   Log into the vCC Node admin Web console as admin.

    The default password is vmware. Check the Web console title to make sure you are configuring the vCC Node.

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

5   When you finish the general configuration tasks, you can exit the vCC Node admin Web console.

System Tab - Node

The **System** tab provides general information on the virtual appliance, allows you to configure times zones, and gives you buttons to shutdown and reboot the appliance.

Information

The main **Information** section provides general information on the virtual appliance, such as the version number and the hostname. It also contains the **Reboot** and **Shutdown** buttons.

Time Zone

The **Time Zone** section allows you to set your local time zone. Click **Time Zone** to see a drop-down menu displaying time zones of the world. Select a time zone and click **Save Settings**.

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

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.

Network Tab - Node

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

Status

The **Network Status** section 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** section allows you to 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 of the displayed fields. In vCD installations, you must set Preferred and Alternate DNS servers manually. Talk to your Service Provider or Network Admin for the appropriate addresses. You recorded the information that you need for these settings in "Collect Necessary Information," on page 12

For more information about network paths in data transfers, see Chapter 3, "Cross-Cloud Data Transfer and Network Connectivity," on page 39

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

Proxy

The **Proxy Settings** section allows you to set up any necessary proxy settings, including address and port. Set this if the appliance must use a proxy to reach systems beyond the firewall at the installation location.

NOTE   Proxies that require a username/password are not supported.

You recorded the information that you need for these settings in "Collect Necessary Information," on page 12

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

Update Tab - Node

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

Status

The **Status** section allows you to view information about your virtual appliance or to check for and install updates. Click **Check Updates** to check for updates from the update repository, shown in the **Available Updates** pane. Click **Install Updates** to install the updates.

Settings

The **Update Settings** section allows you to determine when you want to check for updates. You should leave the **Use Default Repository** button selected. Save any changes you make by clicking **Save Settings**.

Node Tab

On the **Node** tab you can change the Node administrative password, adjust log levels, and manage SSL certificates.

General

In the **General Settings** section you can change the administrative password for the Node.

NOTE   You should change the password for the Node from the default.

You can also set log levels and download logs using this section. Use the drop-down menu to select the log level from TRACE, DEBUG, INFO, WARN, or ERROR and then click **Change Log Level** to save your change. To download a zip of all log files, click **Download logs**.

SSL

In the **Manage SSL Certificates** section you can manage your certificates. vCloud Connector Node includes a self-signed certificate. Before going into production, you must replace that with a valid certificate.

In this section, you can see the certificate currently assigned to your vCloud Connector Node.

Click **Generate and Download CSR** to create a Certificate Signing Request. For more information on installing a valid certificate, see "Add Valid SSL Certificates," on page 35

If you prefer to use your own self-signed certificate, click **Generate and Install**.

Register vCloud Connector Nodes with vCloud Connector Server

You use the vCC Server admin Web console to register vCC Nodes (installed on vSphere or private / public vClouds) with vCC Server. This allows the vCC Server to manage the Nodes.

Prerequisites

The vCC Server admin Web console interface is open.

Procedure

1   Click the **Nodes** tab.

The Manage Nodes page that opens displays the list of Nodes that are currently registered.

2 Click **Register Nodes** and complete the required information.

Option	Description
Name	Enter a name for the cloud where the vCC Node is installed. This name is the display name in the vCC UI.
Type	Select the type of cloud.
FQDN/IP Address	If this is a vSphere cloud, use the IP address of the vCenter Server, such as 192.168.1.101 or the fully qualified domain name. If your vSphere cloud uses a port other than the default 443, indicate that in the address.
	If this is a vCloud Director cloud, use the Organization URL, such as `https://cloud.company.com/cloud/org/orgid`
Public	Select if the cloud is a public cloud outside of the firewall where your vCC Server is installed.
Use Proxy	Select if the vCC Server needs to use a proxy to reach the vCC Node you are registering.
Ignore SSL Certificate	Check if you did not install valid certificates.
	NOTE If you did not install valid certificates, and you do not select this check box, copying fails. If you do select this check box, and later install a valid certificate, you must deselect this check box and restart the server.
IP Address	Type the IP address of the vCC Node to register.
Username	Type an administrative username for the Node admin Web console. The default is admin.
Password	Enter the password for the username: the default is vmware.
Ignore SSL Certificate	Select if you did not install valid certificates.

3 Click **Register**.

The Register Node with Server pop-up window disappears and the vCC Node is now visible in the **Manage Nodes** list. To edit any values or to unregister the Node, click the gear icon at the right of the list entry.

NOTE You should not register a Node with more than one vCC Server.

Register the vCloud Connector UI

You can register the vCloud Connector UI to appear in your vSphere Client, vcloud.vmware.com, or both.

Prerequisites

The vCC Server admin Web console interface is open to the **Server** tab.

Register the vCloud Connector UI in vSphere Client

Set up the vCC UI as a plug-in in vSphere Client using the vCC Server admin Web console.

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

Prerequisites

You need the information you collected in "Collect Necessary Information," on page 12. You need the IP address/fully qualified domain name of the vCC Server and the vCenter Server to which the vSphere Client is pointed. You also need an administrative username and password for that vCenter Server.

Procedure

1 Click the **vSphere Client** button.

2 Fill in the information you collected.

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

NOTE If your vCenter Server is running on a port other than the default 443, make sure you indicate the port along with the IP address.

3 If you have a previously registered version of the Server that you are replacing with this current version, select **Overwrite existing registration**.

4 To create a registration, click **Register**.

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

Registration completed appears in green at the top of the section.

Register the vCloud Connector UI with the vcloud.vmware.com Website

NOTE If you have registered a vCC Server with the website, and you wish to install a new version of vCC Server, you should unregister the current Server from the website before you install the new Server. If you do not do so, the old Server remains registered with vcloud.vmware.com and you cannot delete it. You can still register and use the new Server, but you will have to select that new Server using the Settings page in the UI.

Prerequisites

You need to know the name under which you want your vCC Server to appear at the vcloud.vmware.com website. You need to know the IP address/fully qualified domain name of the vCC Server. You also need to know the vmware.com account username and password you want to use to access the vCC UI through vcloud.vmware.com.

Procedure

1 Click the **vcloud.vmware.com** button.

2 Fill in the information you collected.

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

3 If you want to use SSL to connect your vCC Server instance to the vCC UI appearing in the Web site, check **Use SSL**.

You must have valid certificates installed to use SSL.

4 To create a new registration, click **Register**. To unregister a previous registration, click **Unregister**. To update an existing registration, click **Update Registration**.

Registration completed appears in green at the top of the section.

Prepare vCloud Connector for Production Use

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

Procedure

1 Add Valid SSL Certificates on page 35

If you have not yet replaced the self-signed certificates in your vCC Server and vCC Nodes, you need to do so before production use.

2 Add Multiple Intermediate Certificates on page 35

The admin Web console supports uploading only a single root or intermediate certificate. To upload multiple root/intermediate certificates you must use the command line interface.

3 Configure vCC Node Allocated Storage on page 36

Copy operations rely on staging storage when you copy resources between clouds. To successfully copy resources, make sure you have enough storage in your vSphere and vCloud Director clouds.

Add Valid SSL Certificates

If you have not yet replaced the self-signed certificates in your vCC Server and vCC Nodes, you need to do so before production use.

Procedure

1 Log in to the admin Web console for each vCC instance in which you are going to replace the certificate.

2 For vCC Server, click on the **Server** tab, **SSL** button. For vCC Node, click on the **Node** tab, **SSL** button.

3 Generate and download a Certificate Signing Request by clicking **Generate and Download CSR**.

Depending on your certificate authority, you might need to create a new private key before you download the CSR. Contact your CA for more information.

a If you need to create a new private key, log in to the console of the Server (hcserver) or Node (hcagent) as root. The default password is vmware.

b At the prompt, change directory to `/usr/local/tcserver/springsource-tc-server-standard/`*`server or agent`*`/conf`.

c Delete the existing private key.

`/usr/java/jre-vmware/bin/keytool -delete -alias` ***`hcserver or hcagent`*** **`-keystore tcserver.jks -storepass`** ***`changeme`***

d Create a new private key.

`/usr/java/jre-vmware/bin/keytool -genkey -keyalg RSA -keysize 2048 -alias` ***`hcserver or hcagent`*** **`-validity 1095 -keystore tcserver.jks -storepass`** ***`changeme`*** **`-keypass`** ***`changeme`***

e Log in to the Server Web admin console and download the CSR as described in Step 1above.

4 When you have your certificates, upload the root or intermediate certificate from your CA and the new X.509 certificate for your instance by using the two **Browse** buttons.

5 Locate the certificates on your local machine and then click **Upload**.

What to do next

Once you have installed the valid certificates, deselect the Ignore SSL Certificate flag in the Node registration window for each Node. See "Register vCloud Connector Nodes with vCloud Connector Server," on page 32 for more information on this flag. For the change to take effect, you must restart the Server.

Add Multiple Intermediate Certificates

The admin Web console supports uploading only a single root or intermediate certificate. To upload multiple root/intermediate certificates you must use the command line interface.

Procedure

1 Log in to the console of the Server (hcserver) or Node (hcagent) as root. The default password is vmware.

2 At the prompt, change directory to `/usr/local/tcserver/springsource-tc-server-standard/`*`server or agent`*`/conf`

3   Import the root certifcate.

```
/usr/java/jre-vmware/bin/keytool -import -trustcacerts -alias root -file <location of
root .cer file> -keystore tcserver.jks -storepass changeme
```

4   Import intermediate certificates.

```
/usr/java/jre-vmware/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 with this step.

5   Import the signed certificate.

```
/usr/java/jre-vmware/bin/keytool -import -trustcacerts -alias hcserver or hcagent -file
<location of .cer file> -keystore tcserver.jks -storepass changeme
```

What to do next

Once you have installed the valid certificates, deselect the Ignore SSL Certificate flag in the Node registration window for each Node. See for more information on this flag. For the change to take effect, you must restart the Server.

Configure vCC 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 in your vSphere and vCloud Director clouds.

Default storage on Nodes is 40 GB. You may need to increase this if you will be copying large VMs or templates or if you will be copying many items simultaneously.

Configure vCC Node Allocated Storage in vSphere

To successfully copy resources to or from a vSphere cloud, you must configure and resize the data disk associated with the Node for that vSphere cloud.

Prerequisites

■   You are a vSphere administrator.

■   You have taken a snapshot of the virtual appliance.

Procedure

1   Log in to the vSphere Client.

2   In the hierarchy tree, select the vCC Node virtual appliance.

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

4   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 **Okay**.

7   Open the console for the vCC Node.

8   Run the following command to resize the disk:

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

Configure vCC Node Allocated Storage in vCloud Director

To successfully copy resources to or from a vCD cloud, you must add disk storage to the Node associated with that cloud.

To add disk storage in vCD, you must add disks.

Prerequisites

You are a vCD Org Adminstrator

Procedure

1   Power down the vCC Node.

2   Click the **My Cloud** tab.

3   Select **VMs** in the left panel.

4   Right-click the console icon of the powered down Node in the center panel and select **Properties**.

5   In the Virtual Machine Properties popup, select the **Hardware** tab.

6   Click the **Add +** button to add an additional disk to the Node.

    Size the disk based on the size of the resources you intend to transfer.

7   Click **OK** to accept the change.

8   Right-click the Node console icon and power on the Node.

9   Right-click the Node console icon and select **Popout Console**.

    If you have not yet installed the VMware Remote Console plug-in, you are prompted to install it.

10 Using the console, log in to the Node as admin.

    The default password is vmware.

11 At the command prompt, type: .

    ```
    ls /dev/sd*
    ```

    A disk is created named something like "sdc".

12 Run the following command to add the new disk.

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

13 Log out of the console.

Cross-Cloud Data Transfer and Network Connectivity

3

vCloud Connector 1.5 manages the transfer of content using a separate component, the vCC Node. Using Nodes allows multipart checkpoint-restart in transfers. This flow affects the way a request moves through the system and on how network connectivity must be set up.

Data Flow in Transfer

The following graphic shows the path a vCC request takes in transferring data from a vSphere to a vCloud Director cloud

Figure 3-1. Cross-Cloud Data Flow
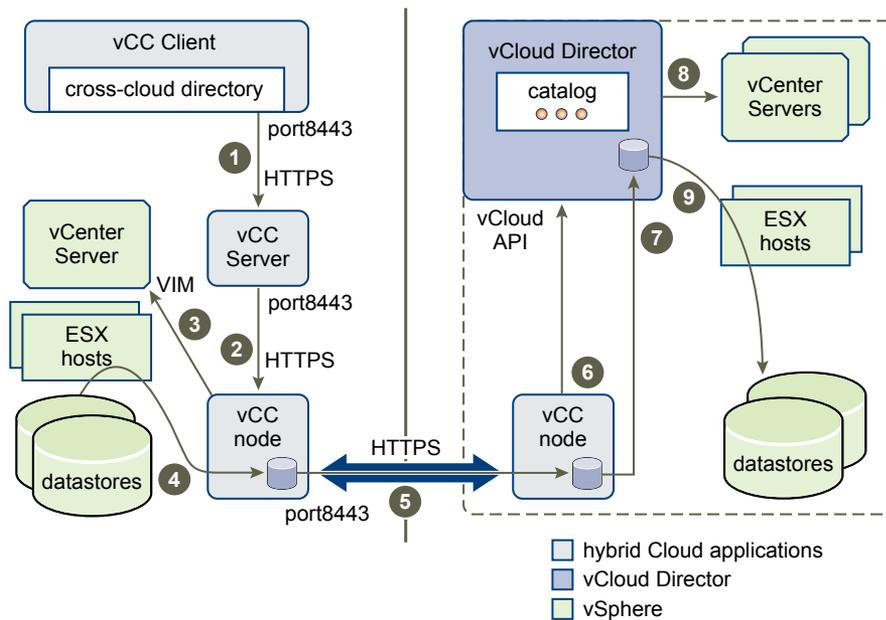
1   Customer requests transfer using vCC UI.

2   vCC Server tells Node to transfer vApp.

3   Node tells vCenter Server to "export" using VIM API.

4   Content is moved from datastores to source Node cache via vmkernel network.

5   Content is transferred from source to destination Node via multipart using checkpoint-restart.

6   Destination Node tells vCD to do an "import" using vCloud API.

7   Content transfers from destination Node cache to vCD transfer server storage.

8   vCD commands the appropriate vCenter import.

9   Content transfers from vCD transfer server storage to destination datastore via vmkernel network and is made available through the vCD catalog.

Troubleshooting vCloud Connector

<div align="right">

4

</div>

Use this information to troubleshoot problems with your vCloud Connector installation and its integration with vcloud.vmware.com.

■ Troubleshooting Storage on page 41

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 41

You can use cURL to pinpoint connectivity problems among the components of your vCloud Connector installation.

■ Troubleshooting Log Access on page 42

The best and easiest way to access log files for a vCC Server or Node instance is through the Web admin interface. Sometimes, however, you need to access the logs through the console.

■ Troubleshooting Log File Size on page 42

To modify the size of log files or the number of files that are retained, you must modify the Server or Node configuration files.

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 during which an interruption occurred, 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 into the appropriate instance as admin either through the console or via SSH. The default password is vmware. The following procedure tests all the connections in order. Use whichever segments are useful to you. Use the -x, --proxy <[protocol://]proxyhost[:port]> option if necessary. If the port number is not specified, it is assumed to be 1080. vCC does not support proxies that require username/password.

Prerequisites

You have installed your vCC Server and Nodes and they are running. You have any necessary proxy information.

Procedure

1   Test the vCC Server connections by logging in to the vCC Server.

2   Test the connection between the vCC Server and a vCD
    cloud:**curl –k –v https://vcd–host/api/versions**

3   Test the connection between the vCC Server and a vCenter Server:**curl –k –v https://vc–host/mob**

4   Test the connection between the vCC Server and a vCC
    Node:**curl –k –v https://node–host:8443/agent/Status**

5   If you are surfacing the vCC UI at vcloud.vmware.com, test the connection between vCC Server and the
    website: **curl –k –v https://vcloud.vmware.com/api/versions**

6   Test the vCC Node connections used in the copy path by first logging into the vCC Node located in the
    vSphere internal cloud.

7   Test the connection between the vCC Node and the vCenter Server:**curl –k –v https://vc–host/mob**

8   Test the connection between the vSphere vCC Node and a vCD vCC Node outside the
    firewall:**curl –k –v https://node–host:8443/agent/Status**

9   Next log into the vCD vCC Node.

10 Test the connection between the vCD vCC Node and the vCD cloud:
    curl –k –v https://vcd–host/api/versions

Troubleshooting Log Access

The best and easiest way to access log files for a vCC Server or Node instance is through the Web admin
interface. Sometimes, however, you need to access the logs through the console.

Server log files are in the hcserver directory. Node log files are in the hcagent directory.

Procedure

1   Open the instance console and log in as admin.

    The default password is vmware.

2   Navigate to /opt/vmware/*hcserver or hcagent*/logs/.

Troubleshooting Log File Size

To modify the size of log files or the number of files that are retained, you must modify the Server or Node
configuration files.

Prerequisites

The original configuration file is backed up.

Procedure

1   Open the running instance console and log in as admin.

    The default password is vmware.

2   For Server, navigate to /usr/local/tcserver/springsource–tc–server–
    standard/server/webapps/hcserver/WEB–INF/classes/logback.xml.

3   For Node, navigate to /usr/local/tcserver/springsource–tc–server–
    standard/*agent*/webapps/agent/WEB–INF/classes/logback.xml

4   Adjust the appropriate values in the following XML snippets:

```
<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.

Index