vCloud Director Installation and Upgrade Guide

vCloud Director 8.10

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-002065-00

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

vCloud Director Installation and Upgrade Guide

The *vCloud Director Installation and Upgrade Guide*provides information about installing or upgrading VMware vCloud Director software and configuring it to work with VMware vSphere®.

Intended Audience

The *vCloud Director Installation and Upgrade Guide* is intended for anyone who wants to install or upgrade VMware vCloud Director software. The information in this book is written for experienced system administrators who are familiar with Linux, Windows, IP networks, and VMware vSphere®.

Overview of vCloud Director Installation, Configuration, and Upgrade

1

A VMware vCloud® combines a vCloud Director server group with the vSphere platform. You create a vCloud Director server group by installing vCloud Director software on one or more servers, connecting the servers to a shared database, and integrating the vCloud Director server group with vSphere.

The initial configuration of vCloud Director, including database and network connection details, is established during installation. When you upgrade an existing installation to a new version of vCloud Director, you update the vCloud Director software and database schema, leaving the existing relationships between servers, the database, and vSphere in place.

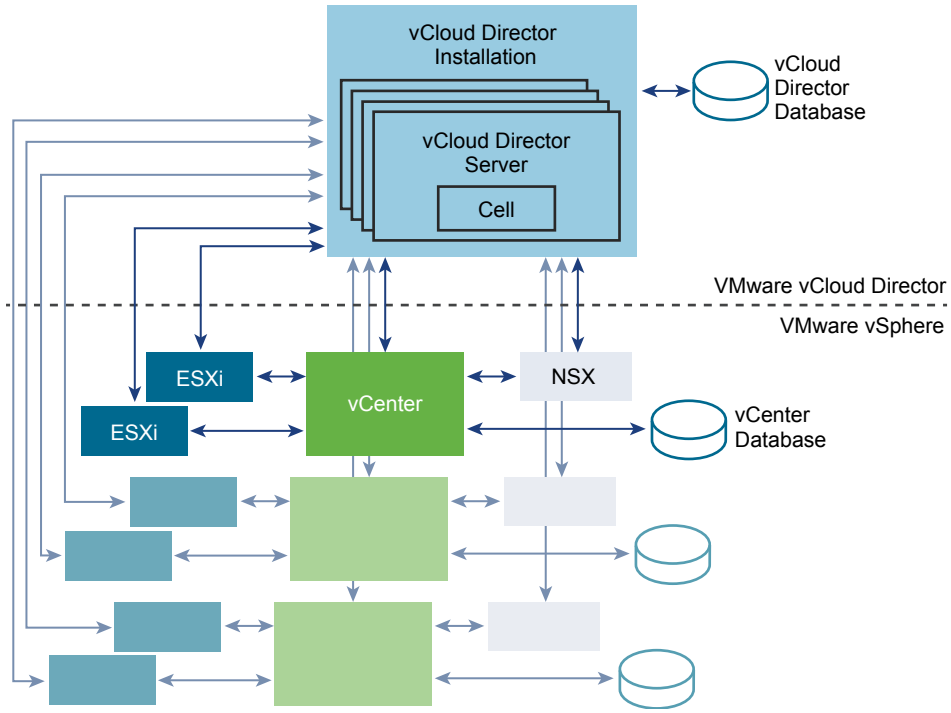
This chapter includes the following topics:

vCloud Director Architecture

A vCloud Director server group consists of one or more vCloud Director servers. These servers share a common database, and are linked to an arbitrary number of vCenter Server systems and ESXi hosts. Network services are provided to the vCenter Server systems and vCloud Director by the VMware NSX Manager™ component from VMware NSX™ for vSphere®.

A typical installation creates a vCloud Director server group comprising several servers. Each server in the group runs a collection of services called a vCloud Director cell. All members of the group share a single database. Each cell in the group connects to multiple vCenter Server systems, the hosts that they manage, and each NSX Manager that is configured to support each connected vCenter Server system.

Figure 1-1. vCloud Director Architecture Diagram



The vCloud Director installation and configuration process creates the cells, connects them to the shared database, and establishes the first connections to a vCenter Server system, that vCenter Server system's associated NSX Manager, and its hosts. A system administrator can then use the vCloud Director Web Console to add vCenter Server systems, the NSX Manager associated with the added vCenter Server system, and the added vCenter Server system's hosts to the vCloud Director server group at any time.

Configuration Planning

vSphere provides storage, compute, and networking capacity to vCloud Director. Before you begin installation, consider how much vSphere and vCloud Director capacity you need, and plan a configuration that can support it.

Configuration requirements depend on many factors, including the number of organizations in the cloud, the number of users in each organization, and the activity level of those users. The following guidelines can serve as a starting point for most configurations:

- Allocate one vCloud Director server (cell) for each vCenter Server system that you want to make accessible in your cloud.
- Be sure that all vCloud Director servers meet at least the minimum requirements for memory and storage detailed in "vCloud Director Hardware and Software Requirements," on page 9.
- Configure the vCloud Director database as described in "Installing and Configuring a vCloud Director Database," on page 12.

vCloud Director Hardware and Software Requirements

Each server in a vCloud Director server group must meet certain hardware and software requirements. In addition, a supported database must be accessible to all members of the group. Each server group requires access to a vCenter server, NSX Manager, and one or more ESXi hosts.

Compatibility With Other VMware Products

For the most recent information about compatibility between vCloud Director and other VMware products, see the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

vSphere Configuration Requirements

VMware vSphere ® servers and ESXi hosts intended for use with vCloud Director must meet specific configuration requirements.

- vCenter networks intended for use as vCloud Director external networks or network pools must be available to all hosts in any cluster intended for vCloud Director to use. Making these networks available to all hosts in a datacenter simplifies the task of adding new vCenter servers to vCloud Director.
- vSphere Distributed Switches are required for isolated networks and network pools.
- vCenter clusters used with vCloud Director must specify a vSphere DRS automation level of **Fully Automated**. Storage DRS, if enabled, can be configured with any automation level.
- vCenter servers must trust their hosts. All hosts in all clusters managed by vCloud Director must be configured to require verified host certificates. In particular, you must determine, compare, and select matching thumbprints for all hosts. See Configure SSL Settings in the *vCenter Server and Host Management* documentation.

vSphere Licensing Requirements

The vCloud Director Service Provider Bundle includes the necessary vSphere licenses.

Supported Platforms, Databases, and Browsers

See the *vCloud Director Release Notes* for information about the server platforms, browsers, LDAP servers, and databases supported by this release of vCloud Director.

Summary of Network Configuration Requirements for vCloud Director

Secure, reliable operation of vCloud Director depends on a secure, reliable network that supports forward and reverse lookup of hostnames, a network time service, and other services. Your network must meet these requirements before you begin installing vCloud Director.

The network that connects vCloud Director servers, the database server, vCenter servers, and the associated vCloud Networking and Security or NSX for vSphere components, must meet several requirements:

IP addresses

Each vCloud Director server must support two different SSL endpoints. One endpoint is for the HTTP service. The other is for the console proxy service. These endpoints can be separate IP addresses, or a single IP address with two different ports. You can use IP aliases or multiple network interfaces to create these addresses. You cannot use the Linux `ip addr add` command to create the second address.

Console Proxy Address

The IP address configured as the console proxy endpoint must not be located behind an SSL-terminating load balancer or reverse proxy. All console proxy requests must be relayed directly to the console proxy IP address.

Network Time Service

You must use a network time service such as NTP to synchronize the clocks of all vCloud Director servers, including the database server. The maximum allowable drift between the clocks of synchronized servers is 2 seconds.

Server Time Zones

All vCloud Director servers, including the database server, must be configured to be in the same time zone.

Hostname Resolution

All host names that you specify during installation and configuration must be resolvable by DNS using forward and reverse lookup of the fully qualified domain name or the unqualified hostname. For example, for a host named `vcloud.example.com`, both of the following commands must succeed on a vCloud Director host:

```
nslookup vcloud
nslookup vcloud.example.com
```

In addition, if the host `vcloud.example.com` has the IP address 192.168.1.1, the following command must return `vcloud.example.com`:

```
nslookup 192.168.1.1
```

Transfer Server Storage

To provide temporary storage for uploads, downloads, and catalog items that are published or subscribed externally, you must make an NFS or other shared storage volume accessible to all servers in a vCloud Director server group. When NFS is used for the transfer server storage, certain configuration settings must set so that each vCloud Director cell in the vCloud Director server group can mount and use the NFS-based transfer server storage. See http://kb.vmware.com/kb/2086127 for details. Each member of the server group must mount this volume at the same mountpoint, typically `/opt/vmware/vcloud-director/data/transfer`. Space on this volume is consumed in two ways:

- Transfers (uploads and downloads) occupy this storage for as long as the transfer is in progress, and are removed when the transfer is complete. Transfers that make no progress for 60 minutes are marked as expired and cleaned up by the system. Because transferred images can be large, it is a good practice to allocate at least several hundred gigabytes for this use.

- Catalog items in catalogs that are published externally and enable caching of published content occupy this storage for as long as they exist. (Items from catalogs that are published externally but do not enable caching do not occupy this storage.) If you enable organizations in your cloud to create catalogs that are published externally, it is safe to assume that hundreds or even thousands of catalog items will need space on this volume, and that each catalog item will be the size of a virtual machine in compressed OVF form.

NOTE If possible, the volume you use for transfer server storage should be one whose capacity can be easily expanded.

Network Security Recommendations

Secure operation of vCloud Director requires a secure network environment. Configure and test this network environment before you begin installing vCloud Director

Connect all vCloud Director servers to a network that is secured and monitored. vCloud Director network connections have several additional requirements:

- Do not connect vCloud Director directly to the public Internet. Always protect vCloud Director network connections with a firewall. Only port 443 (HTTPS) must be open to incoming connections. Ports 22 (SSH) and 80 (HTTP) can also be opened for incoming connections if needed. In addition, the `cell-management-tool` requires access to the cell's loopback address. All other incoming traffic from a public network must be rejected by the firewall.

Table 1-1. Ports That Must Allow Incoming Packets From vCloud Director Hosts

Port	Protocol	Comments
111	TCP, UDP	NFS portmapper used by transfer service
920	TCP, UDP	NFS rpc.statd used by transfer service
61611	TCP	AMQP
61616	TCP	AMQP

- Do not connect the ports used for outgoing connections to the public network.

Table 1-2. Ports That Must Allow Outgoing Packets From vCloud Director Hosts

Port	Protocol	Comments
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	NFS portmapper used by transfer service
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	vCenter, NSX Manager, and ESXi connections
514	UDP	Optional. Enables syslog use.
902	TCP	vCenter and ESXi connections.
903	TCP	vCenter and ESXi connections.
920	TCP, UDP	NFS rpc.statd used by transfer service.
1433	TCP	Default Microsoft SQL Server database port.

Table 1-2. Ports That Must Allow Outgoing Packets From vCloud Director Hosts (Continued)

Port	Protocol	Comments
1521	TCP	Default Oracle database port.
5672	TCP, UDP	Optional. AMQP messages for task extensions.
61611	TCP	AMQP
61616	TCP	AMQP

- Route traffic between vCloud Director servers and the vCloud Director database server over a dedicated private network if possible.
- Virtual switches and distributed virtual switches that support provider networks must be isolated from each other. They cannot share the same level 2 physical network segment.

Installing and Configuring a vCloud Director Database

vCloud Director cells use a database to store shared information. This database must exist before you can complete installation and configuration of vCloud Director software.

NOTE Regardless of the database software you choose, you must create a separate, dedicated database schema for vCloud Director to use. vCloud Director cannot share a database schema with any other VMware product.

Configure an Oracle Database

Oracle databases have specific configuration requirements when you use them with vCloud Director. Install and configure a database instance and create the vCloud Director database user account before you install vCloud Director.

Procedure

1 Configure the database server.

   A database server configured with 16GB of memory, 100GB storage, and 4 CPUs should be adequate for most vCloud Director clusters.

2 Create the database instance.

   Use a command of the following form to create a single CLOUD_DATA tablespace:

   ```
   Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1500M
   autoextend on;
   ```

3 Create the vCloud Director database user account.

   The following command creates database user name `vcloud` with password `vcloudpass`.

   ```
   Create user $vcloud identified by $vcloudpass default tablespace CLOUD_DATA;
   ```

   NOTE When you create the vCloud Director database user account, you must specify CLOUD_DATA as the default tablespace.

4 Configure database connection, process, and transaction parameters.

The database must be configured to allow at least 75 connections per vCloud Director cell plus about 50 for Oracle's own use. You can obtain values for other configuration parameters based on the number of connections, where *C* represents the number of cells in your vCloud Director cluster.

Oracle Configuration Parameter	Value for *C* Cells
CONNECTIONS	75*C+50
PROCESSES	= CONNECTIONS
SESSIONS	= PROCESSES*1.1+5
TRANSACTIONS	= SESSIONS*1.1
OPEN_CURSORS	= SESSIONS

5 Create the vCloud Director database user account.

Do not use the Oracle system account as the vCloud Director database user account. You must create a dedicated user account for this purpose. Grant the following system privileges to the account:

- CONNECT
- RESOURCE
- CREATE TRIGGER
- CREATE TYPE
- CREATE VIEW
- CREATE MATERIALIZED VIEW
- CREATE PROCEDURE
- CREATE SEQUENCE

6 Note the database service name so you can use it when you configure network and database connections.

To find the database service name, open the file `$ORACLE_HOME/network/admin/tnsnames.ora` on the database server and look for an entry of the following form:

```
(SERVICE_NAME = orcl.example.com)
```

Configure a Microsoft SQL Server Database

SQL Server databases have specific configuration requirements when you use them with vCloud Director. Install and configure a database instance, and create the vCloud Director database user account before you install vCloud Director.

vCloud Director database performance is an important factor in overall vCloud Director performance and scalability. vCloud Director uses the SQL Server `tmpdb` file when storing large result sets, sorting data, and managing data that is being concurrently read and modified. This file can grow significantly when vCloud Director is experiencing heavy concurrent load. It is a good practice to create the `tmpdb` file on a dedicated volume that has fast read and write performance. For more information about the `tmpdb` file and SQL Server performance, see http://msdn.microsoft.com/en-us/library/ms175527.aspx.

Prerequisites

- You must be familiar with Microsoft SQL Server commands, scripting, and operation.
- To configure Microsoft SQL Server, log on to the SQL Server host computer using administrator credentials. You can configure SQL server to run with the LOCAL_SYSTEM identity, or any identity with the privilege to run a Windows service.

Procedure

1 Configure the database server.

A database server configured with 16GB of memory, 100GB storage, and 4 CPUs should be adequate for most vCloud Director clusters.

2 Specify Mixed Mode authentication during SQL Server setup.

Windows Authentication is not supported when using SQL Server with vCloud Director.

3 Create the database instance.

The following script creates the database and log files, specifying the proper collation sequence.

```
USE [master]
GO
CREATE DATABASE [vcloud] ON PRIMARY
(NAME = N'vcloud', FILENAME = N'C:\vcloud.mdf', SIZE = 100MB, FILEGROWTH = 10% )
LOG ON
(NAME = N'vcdb_log', FILENAME = N'C:\vcloud.ldf', SIZE = 1MB, FILEGROWTH = 10%)
COLLATE Latin1_General_CS_AS
GO
```

The values shown for SIZE are suggestions. You might need to use larger values.

4 Set the transaction isolation level.

The following script sets the database isolation level to READ_COMMITTED_SNAPSHOT.

```
USE [vcloud]
GO
ALTER DATABASE [vcloud] SET SINGLE_USER WITH ROLLBACK IMMEDIATE;
ALTER DATABASE [vcloud] SET ALLOW_SNAPSHOT_ISOLATION ON;
ALTER DATABASE [vcloud] SET READ_COMMITTED_SNAPSHOT ON WITH NO_WAIT;
ALTER DATABASE [vcloud] SET MULTI_USER;
GO
```

For more about transaction isolation, see http://msdn.microsoft.com/en-us/library/ms173763.aspx.

5 Create the vCloud Director database user account.

The following script creates database user name `vcloud` with password `vcloudpass`.

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
   DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

6 Assign permissions to the vCloud Director database user account.

The following script assigns the `db_owner` role to the database user created in Step 5.

```
USE [vcloud]
GO
sp_addrolemember [db_owner], [vcloud]
GO
```

Create SSL Certificates

vCloud Director uses SSL to secure communications between clients and servers. Before you install and configure a vCloud Director server group, you must create two certificates for each member of the group and import the certificates into host keystores.

Each vCloud Director server must support two different SSL endpoints. These endpoints can be separate IP address, or a single IP address with two different ports. Each endpoint requires its own SSL certificate. Certificates for both endpoints must include an X.500 distinguished name. Many certificate authorities recommend including an X.509 Subject Alternative Name extension in certificates they grant. vCloud Director does not require certificates to include a Subject Alternative Name.

Procedure

1 List the IP addresses for this server.

   Use a command like `ifconfig` to discover this server's IP addresses.

2 For each IP address, run the following command to retrieve the fully qualified domain name to which the IP address is bound.

   `nslookup` *`ip-address`*

3 Make a note of each IP address, the fully qualified domain name associated with it, and whether vCloud Director should use the address for the HTTP service or the console proxy service.

   You need the fully qualified domain names when you create the certificates, and the IP addresses when you configure network and database connections. If the IP address can be reached by other fully qualified domain names, make a note of those too, since you will need to supply them if you want the certificate to include a Subject Alternative Name.

4 Create the certificates.

   You can use certificates signed by a trusted certification authority, or self-signed certificates.

NOTE Signed certificates provide the highest level of trust.

Create and Import a Signed SSL Certificate

Signed certificates provide the highest level of trust for SSL communications.

Each vCloud Director server requires two SSL certificates, one for the HTTP service and one for the console proxy service, in a Java keystore file. You can use certificates signed by a trusted certification authority, or self-signed certificates. Signed certificates provide the highest level of trust.

IMPORTANT These examples specify a 2,048-bit key size, but you should evaluate your installation's security requirements before choosing an appropriate key size. Key sizes less than 1,024 bits are no longer supported per NIST Special Publication 800-131A.

To create and import self-signed certificates, see "Create a Self-Signed SSL Certificate," on page 18.

Prerequisites

- Generate a list of fully-qualified domain names and their associated IP addresses on this server.
- Choose an address to use for the HTTP service and an address to use for the console proxy service. See "Create SSL Certificates," on page 15.
- Verify that you have access to a computer that has a Java version 7 runtime environment, so that you can use the `keytool` command to create the certificate. The vCloud Director installer places a copy of `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`, but you can perform this procedure on any computer that has a Java version 7 runtime environment installed. Certificates created with a `keytool`

from any other source are not supported for use with vCloud Director. Creating and importing the certificates before you install and configure vCloud Director software simplifies the installation and configuration process. These command-line examples assume that `keytool` is in the user's path. The keystore password is represented in these examples as *passwd*.

- Certificates for both endpoints must include an X.500 distinguished name. Many certificate authorities recommend including an X.509 Subject Alternative Name extension in certificates they grant. vCloud Director does not require certificates to include a Subject Alternative Name. Familiarize yourself with the `keytool` command, including its `–dname` and `–ext` options.
- Gather the information required for the argument to the keytool `–dname` option.

Table 1-3. Information required by keytool `–dname` option

X.500 Distinguished Name Subpart	keytool keyword	Description	Example
commonName	CN	The fully qualified domain name associated with the IP address of this endpoint.	CN=vcd1.example.com
organizationalUnit	OU	The name of an organizational unit, such as a department or division, within the organization with which this certificate is associated	OU=Engineering
organizationName	O	The name of the organization with which this certificate is associated	O=Example Corporation
localityName	L	The name of the city or town in which the organization is located.	L=Palo Alto
stateName	S	The name of the state or province in which the organization is located.	S=California
country	C	The name of the country in which the organization is located.	C=US

Procedure

1 Create an untrusted certificate for the HTTP service.

This example command creates an untrusted certificate in a keystore file named `certificates.ks`. The `keytool` options have been placed on separate lines for clarity. The X.500 distinguished name information supplied in the argument to the `–dname` option uses the values shown in the Prerequisites. The DNS and IP values shown in the argument to the `–ext` option are typical. Be sure to include all the DNS names at which this endpoint can be reached, including the one you specified for the `commonName` (CN) value in the `–dname` option argument . You can also include IP addresses, as shown here.

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
```

```
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

IMPORTANT The keystore file and the directory in which it is stored must be readable by the user `vcloud.vcloud`. The vCloud Director installer creates this user and group.

2 Create an untrusted certificate for the console proxy service.

This command adds an untrusted certificate to the keystore file created in Step 1. The `keytool` options have been placed on separate lines for clarity. The X.500 distinguished name information supplied in the argument to the `–dname` option uses the values shown in the Prerequisites. The DNS and IP values shown in the argument to the `–ext` option are typical. Be sure to include all the DNS names at which this endpoint can be reached, including the one you specified for the `commonName` (CN) value in the `–dname` option argument . You can also include IP addresses, as shown here.

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 Create a certificate signing request for the HTTP service.

This command creates a certificate signing request in the file `http.csr`.

```
keytool –keystore certificates.ks –storetype JCEKS –storepass passwd –certreq –alias http –
file http.csr
```

4 Create a certificate signing request for the console proxy service.

This command creates a certificate signing request in the file `consoleproxy.csr`.

```
keytool –keystore certificates.ks –storetype JCEKS –storepass passwd –certreq –alias
consoleproxy –file consoleproxy.csr
```

5 Send the certificate signing requests to your Certification Authority.

If your certification authority requires you to specify a Web server type, use Jakarta Tomcat.

6 When you receive the signed certificates, import them into the keystore file.

   a Import the Certification Authority's root certificate into the keystore file.

   This command imports the root certificate from the `root.cer` file to the `certificates.ks` keystore file.

   ```
   keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias root
   –file root.cer
   ```

   b (Optional) If you received intermediate certificates, import them into the keystore file.

   This command imports intermediate certificates from the `intermediate.cer` file to the `certificates.ks` keystore file.

   ```
   keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias
   intermediate –file intermediate.cer
   ```

   c Import the certificate for the HTTP service.

   This command imports the certificate from the `http.cer` file to the `certificates.ks` keystore file.

   ```
   keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias http
   –file http.cer
   ```

   d Import the certificate for the console proxy service.

   This command imports the certificate from the `consoleproxy.cer` file to the `certificates.ks` keystore file.

   ```
   keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias
   consoleproxy –file consoleproxy.cer
   ```

7 To verify that all the certificates are imported, list the contents of the keystore file.

   ```
   keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –list
   ```

8 Repeat this procedure on all vCloud Director servers in the server group.

What to do next

If you created the `certificates.ks` keystore file on a computer other than the server on which you generated the list of fully qualified domain names and their associated IP addresses, copy the keystore file to that server now. You will need the keystore path name when you run the configuration script. See "Configure Network and Database Connections," on page 26.

Create a Self-Signed SSL Certificate

Self-signed certificates can provide a convenient way to configure SSL for vCloud Director in environments where trust concerns are minimal.

Each vCloud Director server requires two SSL certificates, one for the HTTP service and one for the console proxy service, in a Java keystore file. You can use certificates signed by a trusted certification authority, or self-signed certificates. Signed certificates provide the highest level of trust.

IMPORTANT These examples specify a 2,048-bit key size, but you should evaluate your installation's security requirements before choosing an appropriate key size. Key sizes less than 1,024 bits are no longer supported per NIST Special Publication 800-131A.

To create and import signed certificates, see "Create and Import a Signed SSL Certificate," on page 15.

Prerequisites

- Generate a list of fully-qualified domain names and their associated IP addresses on this server.

- Choose an address to use for the HTTP service and an address to use for the console proxy service. See "Create SSL Certificates," on page 15.
- Verify that you have access to a computer that has a Java version 7 runtime environment, so that you can use the `keytool` command to create the certificate. The vCloud Director installer places a copy of `keytool` in `/opt/vmware/vcloud-director/jre/bin/keytool`, but you can perform this procedure on any computer that has a Java version 7 runtime environment installed. Certificates created with a `keytool` from any other source are not supported for use with vCloud Director. Creating and importing the certificates before you install and configure vCloud Director software simplifies the installation and configuration process. These command-line examples assume that `keytool` is in the user's path. The keystore password is represented in these examples as *passwd*.
- Certificates for both endpoints must include an X.500 distinguished name. Many certificate authorities recommend including an X.509 Subject Alternative Name extension in certificates they grant. vCloud Director does not require certificates to include a Subject Alternative Name. Familiarize yourself with the `keytool` command, including its `-dname` and `-ext` options.
- Gather the information required for the argument to the keytool `-dname` option.

Table 1-4. Information required by keytool `-dname` option

X.500 Distinguished Name Subpart	keytool keyword	Description	Example
commonName	CN	The fully qualified domain name associated with the IP address of this endpoint.	CN=vcd1.example.com
organizationalUnit	OU	The name of an organizational unit, such as a department or division, within the organization with which this certificate is associated	OU=Engineering
organizationName	O	The name of the organization with which this certificate is associated	O=Example Corporation
localityName	L	The name of the city or town in which the organization is located.	L=Palo Alto
stateName	S	The name of the state or province in which the organization is located.	S=California
country	C	The name of the country in which the organization is located.	C=US

Procedure

1 Create an untrusted certificate for the HTTP service.

This example command creates an untrusted certificate in a keystore file named `certificates.ks`. The `keytool` options have been placed on separate lines for clarity. The X.500 distinguished name information supplied in the argument to the `-dname` option uses the values shown in the Prerequisites. The DNS and IP values shown in the argument to the `-ext` option are typical. Be sure to include all the DNS names at which this endpoint can be reached, including the one you specified for the `commonName` (CN) value in the `-dname` option argument . You can also include IP addresses, as shown here.

```
keytool
   -keystore certificates.ks
   -alias http
   -storepass passwd
   -keypass passwd
   -storetype JCEKS
```

```
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

IMPORTANT The keystore file and the directory in which it is stored must be readable by the user `vcloud.vcloud`. The vCloud Director installer creates this user and group.

2 Create an untrusted certificate for the console proxy service.

This command adds an untrusted certificate to the keystore file created in Step 1. The `keytool` options have been placed on separate lines for clarity. The X.500 distinguished name information supplied in the argument to the `–dname` option uses the values shown in the Prerequisites. The DNS and IP values shown in the argument to the `–ext` option are typical. Be sure to include all the DNS names at which this endpoint can be reached, including the one you specified for the `commonName` (CN) value in the `–dname` option argument . You can also include IP addresses, as shown here.

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 To verify that all the certificates are imported, list the contents of the keystore file.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –list
```

4 Repeat this procedure on all vCloud Director servers in the server group.

What to do next

If you created the `certificates.ks` keystore file on a computer other than the server on which you generated the list of fully qualified domain names and their associated IP addresses, copy the keystore file to that server now. You will need the keystore path name when you run the configuration script. See "Configure Network and Database Connections," on page 26.

Install and Configure NSX Manager for a New vCloud Director Installation

vCloud Director requires NSX Manager to provide network services to the cloud. Before you perform a new installation of vCloud Director, you must install and configure NSX Manager and associate a unique instance of NSX Manager with each vCenter Server that you plan to include in your vCloud Director installation.

NSX Manager is included in the VMware NSX for vSphere download. For the most recent information about compatibility between vCloud Director and other VMware products, see the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. For information about the network requirements, see "vCloud Director Hardware and Software Requirements," on page 9.

IMPORTANT This procedure applies only when you are performing a new installation of vCloud Director. If you are upgrading an existing installation of vCloud Director, see Chapter 3, "Upgrading vCloud Director," on page 39.

Prerequisites

- Verify that each of your vCenter Server systems meets the prerequisites for installing NSX Manager.
- Perform the installation task for the NSX Manager virtual appliance described in the *NSX Installation and Upgrade Guide*.

Procedure

1. Log in to the NSX Manager virtual appliance that you installed and confirm the settings that you specified during installation.
2. Associate the NSX Manager virtual appliance that you installed with the vCenter Server system that you plan to add to vCloud Director in your planned vCloud Director installation.

What to do next

Configure VXLAN support in the associated NSX Manager. vCloud Director creates VXLAN network pools to provide network resources to Provider VDCs. If VXLAN support is not configured in the associated NSX Manager, Provider VDCs show a network pool error, and you must create a different type of network pool and associate it with the Provider VDC. For details about configuring VXLAN support, see the *NSX Administration Guide*.

Installing and Configuring an AMQP Broker

AMQP, the Advanced Message Queuing Protocol, is an open standard for message queuing that supports flexible messaging for enterprise systems. vCloud Director includes an AMQP service that you can configure to work with an AMQP broker, such as RabbitMQ, to provide cloud operators with a stream of notifications about events in the cloud. If you want to use this service, you must install and configure an AMQP broker.

While use of an AMQP broker with vCloud Director is optional, a number of integrations use AMQP to communicate with vCloud Director. Consult the installation and configuration documents for any integrations you plan to use.

Procedure

1. Download the RabbitMQ Server from http://info.vmware.com/content/12834_rabbitmq.
2. Follow the RabbitMQ installation instructions to install RabbitMQ on any convenient host.

   The RabbitMQ server host must be reachable on the network by each vCloud Director cell.
3. During the RabbitMQ installation, make a note of the values that you will need to supply when configuring vCloud Director to work with this RabbitMQ installation.
   - The fully-qualified domain name of the RabbitMQ server host, for example `amqp.example.com`.
   - A username and password that are valid for authenticating with RabbitMQ.
   - The port at which the broker listens for messages. The default is `5672`.
   - The RabbitMQ virtual host. The default is "/".

What to do next

By default, the vCloud Director AMQP service sends unencrypted messages. If you configure it to encrypt these messages using SSL, it verifies the broker's certificate by using the default JCEKS trust store of the Java runtime environment on the vCloud Director server. The Java runtime environment is typically located in the `$JRE_HOME/lib/security/cacerts` directory.

To use SSL with the vCloud Director AMQP service, select **Use SSL** on the AMQP Broker Settings section of the Extensibility page of the vCloud Director Web console, and provide either of the following:

- an SSL certificate pathname
- a JCEKS trust store pathname and password

If you do not need to validate the AMQP broker's certificate, you can select **Accept all certificates**.

Download and Install the VMware Public Key

The installation file is digitally signed. To verify the signature, you must download and install the VMware public key.

You can use the Linux `rpm` tool and the VMware public key to verify the digital signature of the vCloud Director installation file, or any other signed downloaded file from `vmware.com`. If you install the public key on the computer where you plan to install vCloud Director, the verification happens as part of the installation or upgrade. You can also manually verify the signature before you begin the installation or upgrade procedure, then use the verified file for all installations or upgrades.

NOTE The download site also publishes a checksum value for the download. The checksum is published in two common forms. Verifying the checksum verifies that the file contents that you downloaded are the same as the contents that were posted. It does not verify the digital signature.

Procedure

1 Create a directory to store the VMware Packaging Public Keys.

2 Use a Web browser to download all of the VMware Public Packaging Public Keys from the http://packages.vmware.com/tools/keys directory.

3 Save the key files to the directory that you created.

4 For each key that you download, run the following command to import the key.

```
# rpm --import /key_path/key_name
```

key_path is the directory in which you saved the keys.

key_name is the filename of a key.

Creating a vCloud Director Server Group

2

A vCloud Director server group consists of one or more vCloud Director servers that share a common database and other configuration details. To create a server group, you install and configure vCloud Director software on the first member of the group. Installation and configuration of the first group member creates a response file that you use to configure additional members of the group.

Prerequisites for Creating a vCloud Director Server Group

IMPORTANT This procedure is for new installations only. If you are upgrading an existing vCloud Director installation, see Chapter 3, "Upgrading vCloud Director," on page 39

Before you begin installing and configuring vCloud Director, complete all of the following tasks.

1. Verify that a supported vCenter Server system is running and properly configured for use with vCloud Director. For supported versions and configuration requirements, see "Compatibility With Other VMware Products," on page 9.
2. Verify that a supported version of NSX Manager is running, associated with the vCenter Server system, and properly configured for use with vCloud Director. For supported NSX versions, see the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. For NSX installation and configuration details, see "Install and Configure NSX Manager for a New vCloud Director Installation," on page 20.
3. Verify that you have at least one server platform that is supported for running the vCloud Director software and that server platform is configured with an appropriate amount of memory and storage. For supported platforms and configuration requirements, see the *vCloud Director Release Notes* .
   - Each member of a server group must support two different SSL endpoints. One endpoint is for the HTTP service. The other is for the console proxy service. These endpoints can be separate IP addresses, or a single IP address with two different ports.
   - Each server must have an SSL certificate for each endpoint. All directories in the pathname to the SSL certificates must be readable by any user. See "Create SSL Certificates," on page 15.
   - For the transfer service, each server must mount an NFS or other shared storage volume at `/opt/vmware/vcloud-director/data/transfer`. This volume must be accessible to all members of the server group. See "Summary of Network Configuration Requirements for vCloud Director," on page 10.
   - Each server should have access to a Microsoft Sysprep deployment package. See "Install Microsoft Sysprep Files on the Servers," on page 35.

4 Verify that you have created a vCloud Director database and that it is accessible to all servers in the group. For a list of supported database software, see the *vCloud Director Release Notes*.

   - Verify that you have created a database account for the vCloud Director database user and that the account has all required database privileges. See "Installing and Configuring a vCloud Director Database," on page 12.
   - Verify that the database service starts when the database server is rebooted.

5 Verify that all vCloud Director servers, the database server, all vCenter Server systems, and those vCenter Server systems' associated NSX Manager components can resolve each other's names as described in "Summary of Network Configuration Requirements for vCloud Director," on page 10.

6 Verify that all vCloud Director servers and the database server are synchronized to a network time server with the tolerances noted in "Summary of Network Configuration Requirements for vCloud Director," on page 10.

7 If you plan to import users or groups from an LDAP service, verify that the service is accessible to each vCloud Director server.

8 Open firewall ports as shown in "Network Security Recommendations," on page 11. Port 443 must be open between vCloud Director and vCenter Server systems.

This chapter includes the following topics:

Install and Configure vCloud Director Software on the First Member of a Server Group

All members of a vCloud Director share database connection and other configuration details that you specify when installing and configuring the first member of the group. These details are captured in a response file that you must use when adding members to the group.

vCloud Director software is distributed as a digitally signed Linux executable file with a name of the form `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, where *v.v.v* represents the product version and *nnnnnn* the build number. For example: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Running this executable installs or upgrades vCloud Director.

The vCloud Director installer verifies that the target server meets all platform prerequisites and installs vCloud Director software on it. After the software is installed on the target server, you must run a script that configures the server's network and database connections. This script creates a response file that you must use when configuring additional members of this server group.

Prerequisites

- Verify that the target server and the network it connects to meet the requirements specified in "Summary of Network Configuration Requirements for vCloud Director," on page 10.
- Verify that you have superuser credentials for the target server.
- Verify that the target server mounts the shared transfer service storage volume at `/opt/vmware/vcloud-director/data/transfer`.

- To have the installer verify the digital signature of the installation file, download and install the VMware public key on the target server. If you already verified the digital signature of the installation file, you do not need to verify it again during installation. See "Download and Install the VMware Public Key," on page 22.

Procedure

1 Log in to the target server as root.

2 Download the installation file to the target server.

If you purchased the software on a CD or other media, copy the installation file to a location that is accessible to all target servers.

3 Verify that the checksum of the download matches the one posted on the download page.

Values for MD5 and SHA1 checksums are posted on the download page. Use the appropriate tool to verify that the checksum of the downloaded installation file matches the one shown on the download page. A Linux command of the following form displays the checksum for *installation-file*.

```
[root@cell1 /tmp]# md5sum installation-file
checksum-value installation-file
```

Compare the *checksum-value* produced by this command with the MD5 checksum copied from the download page.

4 Ensure that the installation file is executable.

The installation file requires execute permission. To be sure that it has this permission, open a console, shell, or terminal window and run the following Linux command, where *installation-file* is the full pathname to the vCloud Director installation file.

```
[root@cell1 /tmp]# chmod u+x installation-file
```

5 In a console, shell, or terminal window, run the installation file.

To run the installation file, type its full pathname, for example:

```
[root@cell1 /tmp]# ./installation-file
```

The file includes an installation script and an embedded RPM package.

NOTE You cannot run the installation file from a directory whose pathname includes any embedded space characters.

The installer prints a warning of the following form if you have not installed the VMware public key on the target server.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

When the installer runs, it takes these actions.

a Verifies that the host meets all requirements

b Verifies the digital signature on the installation file

c Creates the `vcloud` user and group

d Unpacks the vCloud Director RPM package

e Installs the software

After the software is installed, the installer prompts you to run the configuration script, which configures the server's network and database connections.

What to do next

Decide whether to run the configuration script.

- If you have completed the prerequisites listed in "Prerequisites for Creating a vCloud Director Server Group," on page 23, you can run the configuration script now. Type **y** and press Enter.
- If you are not ready to run the configuration script now, type **n** and press Enter to exit to the shell.

For more information about running the configuration script, see "Configure Network and Database Connections," on page 26.

Configure Network and Database Connections

After vCloud Director software is installed on the server, the installer prompts you to run a script that configures the server's network and database connections.

You must install vCloud Director software on the server before you can run the configuration script. The installer prompts you to run the script after installation is finished, but you can choose to run it later.

To run the script after the vCloud Director software is installed, log in as root, open a console, shell, or terminal window, and enter the `configure` command:

```
/opt/vmware/vcloud-director/bin/configure
```

The configuration script creates network and database connections for a single vCloud Director server. The script also creates a response file that preserves database connection information for use in subsequent server installations.

IMPORTANT After you run the configuration script to configure the first member of the server group, you must use the `-r` option and specify the response file pathname when configuring additional members of the group. See "Protecting and Reusing the Response File," on page 33.

You can run the configuration script in either an interactive mode or an unattended mode. This procedure describes interactive configuration. For an example of unattended configuration, see "Example: Unattended Configuration," on page 32.

Prerequisites

- Verify that a database of a supported type is accessible from the vCloud Director server. See "Installing and Configuring a vCloud Director Database," on page 12 and "vCloud Director Hardware and Software Requirements," on page 9.
- Have the following information available:
  - Location and password of the keystore file that includes the SSL certificates for this server. See "Create and Import a Signed SSL Certificate," on page 15. The configuration script does not run with a privileged identity. The keystore file and the directory in which it is stored must be readable by any user.
  - Password for each SSL certificate.
  - Hostname or IP address of the database server.
  - Database name and connection port.
  - Database user credentials (user name and password). This user must have specific database privileges. See "Installing and Configuring a vCloud Director Database," on page 12.
  - Other database-specific details such as the database service name, instance name, and domain. See "Installing and Configuring a vCloud Director Database," on page 12.

Procedure

1 Specify the IP addresses to use for the HTTP and console proxy services running on this host.

Each member of a server group must support two SSL endpoints: one for the HTTP service and another for the console proxy service. To begin the configuration process, choose which of the IP addresses discovered by the script to use as the endpoint for each service.

```
Please indicate which IP address available on this machine should be used
for the HTTP service and which IP address should be used for the remote console proxy.

The HTTP service IP address is used for accessing the user interface and the REST API.
The remote console proxy IP address is used for all remote console (VMRC) connections
and traffic.
Please enter your choice for the HTTP service IP address:
    1: 10.17.118.158
    2: 10.17.118.159
Choice [default=1]:2
Please enter your choice for the remote console proxy IP address
    1: 10.17.118.158
    Choice [default=1]:
```

NOTE If you need to use a single IP address with a port for each service, you must run `configure` in unattended mode. See "Example: Unattended Installation Specifying a Single IP Address," on page 32.

2 Specify the full path to the Java keystore file.

```
Please enter the path to the Java keystore containing your SSL certificates and
private keys:/opt/keystore/certificates.ks
```

3 Enter the keystore and certificate passwords.

```
Please enter the password for the keystore:
Please enter the private key password for the 'http' SSL certificate:
Please enter the private key password for the 'consoleproxy' SSL certificate:
```

4 Configure audit message handling options.

Services in each vCloud Director cell log audit messages to the vCloud Director database, where they are preserved for 90 days. To preserve audit messages longer, you can configure vCloud Director services to send audit messages to the `syslog` utility in addition to the vCloud Director database.

Option	Action
To log audit messages to both `syslog` and the vCloud Director database	Enter the `syslog` host name or IP address.
To log audit messages only to the vCloud Director database	Press **Enter**.

```
If you would like to enable remote audit logging to a syslog
host please enter the hostname or IP address of the syslog server. Audit logs are stored by
vCloud Director for 90 days. Exporting logs via syslog will enable you to
preserve them for as long as necessary.

Syslog host name or IP address [press Enter to skip]:10.150.10.10
```

5 Specify the port on which the `syslog` process monitors the specified server.

The default is port 514.

```
What UDP port is the remote syslog server listening on? The
standard syslog port is 514. [default=514]:
Using default value "514" for syslog port.
```

6 Specify the database type, or press **Enter** to accept the default value.

```
The following database types are supported:
       1. Oracle
       2. Microsoft SQL Server
Enter the database type [default=1]:
Using default value "1" for database type.
```

7 Specify database connection information.

a Enter the host name or IP address of the database server.

```
Enter the host (or IP address) for the database:10.150.10.78
```

b Provide database-specific information.

Some of the information that the script requires depends on your choice of database type.

- Oracle database:
  1. Enter the database port, or press **Enter** to accept the default value.

     ```
     Enter the database port [default=1521]:
     Using default value "1521" for port.
     ```

  2. Enter the database service name.

     ```
     Enter the database service name [default=oracle]:orcl.example.com
     ```

     If you press Enter, the configuration script uses a default value, which might not be correct for some installations. For information about how to find the database service name for an Oracle database, see "Configure an Oracle Database," on page 12.

- Microsoft SQL Server database:
  1. Enter the database port, or press **Enter** to accept the default value.

     ```
     Enter the database port [default=1433]:
     Using default value "1433" for port.
     ```

  2. Enter the database name.

     ```
     Enter the database name [default=vcloud]:
     ```

  3. Enter the database instance, or press **Enter** to use the server's default instance.

     ```
     Enter the database instance [Press enter to use the server's default instance]:
     Using the default instance.
     ```

c Enter the database user name and password.

```
Enter the database username:vcloud
Enter the database password:
```

8 Specify whether this installation participates in the VMware Customer Experience Improvement Program (CEIP).

VMware's Customer Experience Improvement Program ("CEIP") provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical information about your organization's use of VMware products and services on a regular basis in association with your

organization's VMware license key(s). This information does not personally identify any individual. Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. If you prefer not to participate in VMware's CEIP for this product, enter **n** in response to the prompt.

```
VMware's Customer Experience Improvement Program ("CEIP") provides
VMware with information that enables VMware to improve its products and services ...
...
Join the VMware Customer Experience Improvement Program [y/n]:y
```

You may use the cell management tool to join or leave VMware's CEIP for this product at any time. See "Cell Management Tool Reference" in *vCloud Director Administrator's Guide*.

What to do next

The script validates the information that you supplied, then continues with three more steps.

1 It initializes the database and connects this server to it.

2 It offers to start vCloud Director services on this host.

3 It displays a URL at which you can connect to the Setup wizard after vCloud Director service starts.

This fragment shows a typical completion of the script.

```
Connecting to the database: jdbc:oracle:thin:vcloud/vcloud@10.150.10.78:1521/vcloud
..........
Database configuration complete.
Once the vCloud Director server has been started you will be able to
access the first-time setup wizard at this URL:

    http://vcloud.example.com

Would you like to start the vCloud Director service now? If you choose not
to start it now, you can manually start it at any time using this command:
    service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment).

The service was started; it may be several minutes before it is ready for use.
Please check the logs for complete details.

vCloud Director configuration is now complete. Exiting...
```

NOTE Database connection information and other reusable responses that you supplied during configuration are preserved in a file at `/opt/vmware/vcloud-director/etc/responses.properties` on this server. This file contains sensitive information that you must reuse when you add servers to a server group. Preserve the file in a secure location, and make it available only when needed.

To add servers to this group, see "Install vCloud Director Software on Additional Members of a Server Group," on page 34.

After vCloud Director services are running on all servers, you must initialize the server group's database with a license key, system administrator account, and related information. You can initialize the database in one of the following ways:

- Using a Web browser, open the Setup wizard at the URL displayed when the script finishes. See Chapter 4, "vCloud Director Setup," on page 51.

- Use the cell management tool `system-setup` subcommand. See "Cell Management Tool Reference" in *vCloud Director Administrator's Guide*.

Configuration Utility Reference

The vCloud Director configuration utility configures the cell's network and database connections. You can run it in an interactive mode in which the utility prompts you for required information. Or you can run the utility in an unattended mode that requires you to supply all required information at the command line.

If you want to configure vCloud Director without using an interactive procedure, you can run the configuration utility as a single command line, specifying unattended operation. When you run the utility this way, you must supply all the information that the system requires as arguments to command-line options.

Table 2-1. Configuration Utility Options and Arguments

Option	Argument	Description
`--help` (-h)	None	Displays a summary of configuration options and arguments
`--config-file` (-c)	Path to the `global.properties` file	Information that you supply when you run the configuration utility is saved in this file. If you omit this option, the default location,`/opt/vmware/vcloud-director/etc/global.properties`, is used.
`--console-proxy-ip` (-cons)	IPv4 address, with optional port number	The system uses this address for the vCloud Director console proxy service. For example `10.17.118.159`.
`--console-proxy-port-https`	Integer in the range 0 to 65535	Port number to use for the vCloud Director console proxy service
`--database-host` (-dbhost)	IP address or fully qualified domain name of the vCloud Director database host	See "Installing and Configuring a vCloud Director Database" in *vCloud Director Installation and Upgrade Guide*.
`--database-domain` (-dbdomain)	SQL Server database user domain	Optional if database type is `sqlserver`
`--database-instance` (-dbinstance)	SQL Server database instance	Optional if database type is `sqlserver`
`--database-name` (-dbname)	The database service name	See "Installing and Configuring a vCloud Director Database" in *vCloud Director Installation and Upgrade Guide*.
`--database-password` (-dbpassword)	Password for the database user. It can be null.	See "Installing and Configuring a vCloud Director Database" in *vCloud Director Installation and Upgrade Guide*.
`--database-port` (-dbport)	Port number used by the database service on the database host	See "Installing and Configuring a vCloud Director Database" in *vCloud Director Installation and Upgrade Guide*.

Table 2-1. Configuration Utility Options and Arguments (Continued)

Option	Argument	Description
`--database-type` (-dbtype)	The database type. Choose one: ■ oracle ■ sqlserver	See "Installing and Configuring a vCloud Director Database" in *vCloud Director Installation and Upgrade Guide*.
`--database-user` (-dbuser)	User name of the database user.	See "Installing and Configuring a vCloud Director Database" in *vCloud Director Installation and Upgrade Guide*.
`--enable-ceip`	Choose one: ■ true ■ false	Specifies whether this installation participates in the VMware Customer Experience Improvement Program (CEIP). Defaults to true if not provided and not set to false in the current configuration. VMware's Customer Experience Improvement Program ("CEIP") provides Additional information regarding the data collected through CEIP and the purposes for which it is used by VMware is set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. You may use the cell management tool to join or leave VMware's CEIP for this product at any time. See "Cell Management Tool Reference" in *vCloud Director Administrator's Guide*.
`--uuid` (-g)	None	Generates a new unique identifier for the cell
`--primary-ip` (-ip)	IPv4 address, with optional port number	The system uses this address for the vCloud Director Web interface service. For example `10.17.118.159`.
`--primary-port-http`	Integer in the range 0 to 65535	Port number to use for HTTP (insecure) connections to the vCloud Director Web interface service
`--primary-port-https`	Integer in the range 0 to 65535	Port number to use for HTTPS (secure) connections to the vCloud Director Web interface service
`--keystore` (-k)	Path to the Java keystore containing your SSL certificates and private keys	Must be a full path name. For example, `/opt/keystore/certificates.ks` .

Table 2-1. Configuration Utility Options and Arguments (Continued)

Option	Argument	Description
`--syslog-host` (-loghost)	IP address or fully qualified domain name of the syslog server host	Services in each vCloud Director cell log audit messages to the vCloud Director database, where they are preserved for 90 days. To preserve audit messages longer, you can configure vCloud Director services to send audit messages to the `syslog` utility in addition to the vCloud Director database.
`--syslog-port` (-logport)	Integer in the range 0 to 65535	The port on which the `syslog` process monitors the specified server. Defaults to 514 if not specified.
`--response-file` (-r)	Path to the response file	Must be a full path name. Defaults to `/opt/vmware/vcloud-director/etc/responses.properties` if not specified. All the information that you supply when running configure is preserved in this file. IMPORTANT This file contains sensitive information that you must reuse when you add servers to a server group. Preserve the file in a secure location, and make it available only when needed. See "Protecting and Reusing the Response File," on page 33.
`--unattended-installation` (-unattended,)	None	Specifies unattended installation
`--keystore-password` (-w)	SSL certificate keystore password	SSL certificate keystore password

Example: Unattended Configuration

IMPORTANT Before you run the `configure`, verify that the value of the environment variable `VCLOUD_HOME` is set to the full pathname of the directory in which vCloud Director is installed. This value is typically `/opt/vmware/vcloud-director`.

The following command line runs an unattended configuration that specifies the same values that are used in the interactive procedure in "Configure Network and Database Connections," on page 26.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons 10.17.118.158 \
-dbtype oracle -dbhost 10.150.10.78 -dbname orcl.example.com -dbuser vcloud --enable-ceip true \
-dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret -loghost 10.150.10.10 -unattended
```

For more examples and reference information about the command-line options for `configure`, see "Configuration Utility Reference," on page 30.

Example: Unattended Installation Specifying a Single IP Address

IMPORTANT Before you run the `configure`, verify that the value of the environment variable `VCLOUD_HOME` is set to the full pathname of the directory in which vCloud Director is installed. This value is typically `/opt/vmware/vcloud-director`.

The following command line runs an unattended configuration that specifies the same configuration values that are used in "Configure Network and Database Connections," on page 26. This example does not use separate IP addresses for the Web interface service and the console proxy services. Instead, the example specifies a single IP address for both services and uses the `--primary-port-https` and `--console-proxy-port-https` options to designate a different port for each service.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#
./configure -ip 10.17.118.159 --primary-port-https 9000 -cons 10.17.118.159 \
--console-proxy-port-https 9010 -dbtype oracle -dbhost 10.150.10.78 -dbname orcl.example.com \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

Protecting and Reusing the Response File

Network and database connection details that you supply when you configure the first vCloud Director cell are saved in a response file. This file contains sensitive information that you must reuse when you add more servers to a server group. Preserve the file in a secure location, and make it available only when needed.

The response file is created at `/opt/vmware/vcloud-director/etc/responses.properties` on the first server for which you configure network and database connections. When you add more servers to the group, you must use a copy of the response file to supply configuration parameters that all servers share.

IMPORTANT The cell management tool includes subcommands that you can use to make changes in the network and database connection details that you specified when you configured the first vCloud Director cell. Changes you make using these tools are written to the global configuration file and the response file, so you must be sure to have the response file in place (in `/opt/vmware/vcloud-director/etc/responses.properties`) and writable before you use any of the commands that can modify it. . See the "Cell Management Tool Reference" in the *vCloud Director Administrator's Guide*.

Procedure

1 Protect the response file.

  Save a copy of the file in a secure location. Restrict access to it, and make sure it is backed up to a secure location. When you back up the file, avoid sending cleartext across a public network.

2 Reuse the response file.

  a Copy the file to a location accessible to the server you are ready to configure.

  NOTE You must install vCloud Director software on a server before you can reuse the response file to configure it. All directories in the pathname to the response file must be readable by the user `vcloud.vcloud`, as shown in this example.

  ```
  [root@cell1 /tmp]# ls -l responses.properties
  -rw------- 1 vcloud vcloud 418 Jun 8 13:42 responses.properties
  ```

  The installer creates this user and group.

  ---

  b Run the configuration script, using the `-r` option and specifying the response file pathname.

  Log in as root, open a console, shell, or terminal window, and type:

  ```
  [root@cell1 /tmp]# /opt/vmware/vcloud-director/bin/configure -r /path-to-response-file
  ```

What to do next

After you configure the additional servers, delete the copy of the response file you used to configure them.

Install vCloud Director Software on Additional Members of a Server Group

You can add servers to a vCloud Director server group at any time. Because all servers in a server group must be configured with the same database connection details, you must use the response file created when you configured the first member of the group to supply this information when you configure additional members.

Prerequisites

- Verify that you can access the response file that was created when you installed and configured the first member of this server group. See "Protecting and Reusing the Response File," on page 33.
- Verify that the vCloud Director database is accessible from this server.
- Verify that the SSL certificates that you created for this server are installed in a location that the installer can access. See "Create and Import a Signed SSL Certificate," on page 15. The configuration script does not run with a privileged identity, so the keystore file and the path in which it is stored must be readable by any user. Using the same keystore path (for example, `/tmp/certificates.ks`) on all members of a server group simplifies the installation process.
- Have the following information available:
  - The password of the keystore file that includes the SSL certificates for this server.
  - Password for each SSL certificate.

Procedure

1. Log in to the target server as root.
2. Download the installation file to the target server.

   If you purchased the software on a CD or other media, copy the installation file to a location that is accessible to all target servers.
3. Ensure that the installation file is executable.

   The installation file requires execute permission. To be sure that it has this permission, open a console, shell, or terminal window and run the following Linux command, where *installation-file* is the full pathname to the vCloud Director installation file.

   ```
   [root@cell1 /tmp]# chmod u+x installation-file
   ```
4. Copy the response file to a location accessible to this server.

   All directories in the pathname to the response file must be readable by root.
5. In a console, shell, or terminal window, run the installation file using the `-r` option and specifying the response file pathname.

   To run the installation file, type its full pathname, for example:

   ```
   [root@cell1 /tmp]# ./installation-file -r /path-to-response-file
   ```

   The file includes an installation script and an embedded RPM package.

   NOTE You cannot run the installation file from a directory whose pathname includes any embedded space characters.

   The installer prints a warning of the following form if you have not installed the VMware public key on the target server.

   ```
   warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
   ```

When the installer runs with the `-r` option, it takes these actions.

a Verifies that the host meets all requirements

b Verifies the digital signature on the installation file

c Creates the `vcloud` user and group

d Unpacks the vCloud Director RPM package

e Installs the software

f Copies the response file to a location readable by vcloud.vcloud

g Runs the configuration script using the response file as input

When the configuration script runs, it looks for the certificates in the path saved in the response file (for example, `/tmp/certificates.ks`), then prompts you to supply the keystore and certificate passwords. If the configuration script does not find valid certificates in the pathname saved in the response file, it prompts you for a pathname to the certificates.

6 (Optional) Repeat this procedure to add more servers to this server group.

What to do next

If your cloud needs to support guest customization for certain older Microsoft operating systems, install Sysprep files on all members of the server group. See "Install Microsoft Sysprep Files on the Servers," on page 35.

After the configuration script finishes and vCloud Director services are running on all servers, you can open the Setup wizard at the URL that appears when the script completes. See Chapter 4, "vCloud Director Setup," on page 51.

Install Microsoft Sysprep Files on the Servers

Before vCloud Director can perform guest customization on virtual machines with certain older Windows guest operating systems, you must install the appropriate Microsoft Sysprep files on each member of the server group.

Sysprep files are required only for some older Microsoft operating systems. If your cloud does not need to support guest customization for those operating systems, you do not need to install Sysprep files.

To install the Sysprep binary files, you copy them to a specific location on the server. You must copy the files to each member of the server group.

Prerequisites

Verify that you have access to the 32- and 64-bit Sysprep binary files for Windows 2003 and Windows XP.

Procedure

1 Log in to the target server as root.

2 Change directory to `$VCLOUD_HOME/guestcustomization/default/windows`.

```
[root@cell1 /]# cd /opt/vmware/vcloud-director/guestcustomization/default/windows
```

3 Create a directory named `sysprep`.

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep
```

4 For each guest operating system that requires Sysprep binary files, create a subdirectory of `$VCLOUD_HOME/guestcustomization/default/windows/sysprep`.

Subdirectory names are specific to a guest operating system.

Table 2-2. Subdirectory Assignments for Sysprep Files

Guest OS	Subdirectory to Create Under $VCLOUD_HOME/guestcustomization/default/windows/sysprep
Windows 2003 (32-bit)	svr2003
Windows 2003 (64-bit)	svr2003-64
Windows XP (32-bit)	xp
Windows XP (64-bit)	xp-64

For example, to create a subdirectory to hold Sysprep binary files for Windows XP, use the following Linux command.

```
[root@cell1 /opt/vmware/vcloud-director/guestcustomization/default/windows]# mkdir sysprep/xp
```

5 Copy the Sysprep binary files to the appropriate location on each vCloud Director server in the server group.

6 Ensure that the Sysprep files are readable by the user `vcloud.vcloud`.

Use the Linux `chown` command to do this.

```
[root@cell1 /]# chown -R vcloud:vcloud $VCLOUD_HOME/guestcustomization
```

When the Sysprep files are copied to all members of the server group, you can perform guest customization on virtual machines in your cloud. You do not need to restart vCloud Director after the Sysprep files are copied.

Start or Stop vCloud Director Services

After you complete installation and database connection setup on a server, you can start vCloud Director services on it. You can also stop these services if they are running.

The configuration script prompts you to start vCloud Director services. You can let the script start these services for you, or you can start the services yourself later. These services must be running before you can complete and initialize the installation.

vCloud Director services start whenever you reboot a server.

IMPORTANT If you are stopping vCloud Director services as part of a vCloud Director software upgrade, you must use the cell management tool, which allows you to quiesce the cell before stopping services. See the Cell Management Tool Reference in the *vCloud Director Administrator's Guide*.

Procedure

1 Log in to the target server as root.

2 Start or stop services.

Option	Action
Start services	Open a console, shell, or terminal window and run the following command. `service vmware-vcd start`
Stop services when the cell is in use	Use the cell management tool.
Stop services when the cell is not in use	Open a console, shell, or terminal window and run the following command. `service vmware-vcd stop`

Uninstall vCloud Director Software

Use the Linux `rpm` command to uninstall vCloud Director software from an individual server.

Procedure

1 Log in to the target server as root.

2 Unmount the transfer service storage, typically mounted at `/opt/vmware/vcloud-director/data/transfer`.

3 Open a console, shell, or terminal window and run the Linux `rpm` command.

```
rpm –e vmware–vcloud–director vmware–vcloud–director–rhel
```

If other packages are installed that depend on the `vmware–vcloud–director` package, the system will prompt you to uninstall those packages before you uninstall vCloud Director.

Upgrading vCloud Director 3

To upgrade vCloud Director to a new version, install the new version on each server in the vCloud Director server group, upgrade the vCloud Director database, and restart vCloud Director services.

IMPORTANT This upgrade procedure assumes that you are upgrading a vCloud Director installation that includes releases of VMware vSphere ® and VMware NSX ™ that are also compatible with vCloud Director 8.10. Before you begin this procedure, refer to the *VMware Product Interoperability Matrixes* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php for information about the versions of other VMware products that are compatible with the version of vCloud Director that you are currently running and also with vCloud Director 8.10. If you plan to upgrade your installation's vSphere or NSX components as part of the upgrade to vCloud Director 8.10., it is important to upgrade those components in the order and using the procedures documented here.

After you upgrade a vCloud Director server, you must also upgrade its vCloud Director database. The database stores information about the runtime state of the server, including the state of all vCloud Director tasks it is running. To ensure that no invalid task information remains in the database after an upgrade, you must ensure that no tasks are active on the server before you begin the upgrade.

The upgrade also preserves the following artifacts, which are not stored in the vCloud Director database:

- Local and global properties files are copied to the new installation.
- Microsoft sysprep files used for guest customization are copied to the new installation.

Unless you use a load balancer to distribute client requests across members of your vCloud Director server group (see "Using a Load Balancer to Reduce Service Downtime," on page 40), the upgrade requires sufficient vCloud Director downtime to upgrade the database and at least one server.

Upgrading a vCloud Director Server Group

1. Disable user access to vCloud Director. You can also display a maintenance message while the upgrade is underway. See "Displaying the Maintenance Message During an Upgrade," on page 41.
2. Use the cell management tool to quiesce all cells in the server group and shut down vCloud Director services on each server. See the Cell Management Tool Reference in the *vCloud Director Administrator's Guide*.
3. Upgrade vCloud Director software on all members of the server group. See "Upgrade vCloud Director Software on Any Member of a Server Group," on page 42. You can upgrade the servers individually or in parallel, but you must not restart vCloud Director services on any upgraded member of the group before you upgrade the vCloud Director database.
4. Upgrade the vCloud Director database. See "Upgrade the vCloud Director Database," on page 45.
5. Restart vCloud Director on the upgraded servers. See "Start or Stop vCloud Director Services," on page 36.

6 Enable user access to vCloud Director.

7 (Optional) Upgrade each associated NSX Manager. See "Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System," on page 47.

8 (Optional) Upgrade each associated vCenter Server system and its ESXi hosts. See "Upgrade vCenter Server Systems, Hosts, and NSX Edges," on page 47.

NOTE After completing the upgrade, if you have the vCloud Director Web Console open in a browser, log out and clear your browser cache before logging back in to the Web Console.

Using a Load Balancer to Reduce Service Downtime

If you are using a load balancer or other tool that can force requests to go to specific servers, you can upgrade a subset of the server group while keeping existing services available on the remaining subset. This approach reduces vCloud Director service downtime to the length of time required to upgrade the vCloud Director database. Users might experience some degradation of performance during the upgrade, but in-progress tasks continue to run as long as any subset of the server group is operational. Console sessions might be interrupted, but you can restart them.

1 Use the load balancer to redirect vCloud Director requests to a subset of the servers in the group. Follow the procedures recommended by your load balancer.

2 Use the cell management tool to quiesce the cells that are no longer handling requests and shut down vCloud Director services on those servers.

NOTE Console sessions routed through a server's console proxy are interrupted when the server shuts down. Clients can refresh the console window to recover.

See the Cell Management Tool Reference in the *vCloud Director Administrator's Guide*.

3 Upgrade vCloud Director software on the members of the server group on which you have stopped vCloud Director, but do not restart those services. See "Upgrade vCloud Director Software on Any Member of a Server Group," on page 42.

4 Use the cell management tool to quiesce the cells that you have not yet upgraded and shut down vCloud Director services on those servers.

5 Upgrade the vCloud Director database. See "Upgrade the vCloud Director Database," on page 45.

6 Restart vCloud Director on the upgraded servers. See "Start or Stop vCloud Director Services," on page 36.

7 (Optional) Upgrade each associated NSX Manager. See "Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System," on page 47.

8 (Optional) Upgrade each associated vCenter Server system and its ESXi hosts. See "Upgrade vCenter Server Systems, Hosts, and NSX Edges," on page 47.

9 Use the load balancer to redirect vCloud Director requests to the upgraded servers.

10 Upgrade vCloud Director software on the remaining servers in the group, and restart vCloud Director on those servers as the upgrades complete. See "Upgrade vCloud Director Software on Any Member of a Server Group," on page 42.

Displaying the Maintenance Message During an Upgrade

If you anticipate a lengthy upgrade process and want to have the system display a maintenance message while the upgrade is underway, verify that at least one cell remains accessible while the others are being upgraded. Run the `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` command on that cell to turn on the cell maintenance message.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
```

When you are ready to return an upgraded cell to service, run the following command on the cell to turn off the maintenance message.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# service vmware-vcd restart
```

This chapter includes the following topics:

Use the Cell Management Tool to Quiesce and Shut Down a Server

Before you upgrade a vCloud Director server, use the cell management tool to quiesce and shut down vCloud Director services on the server's cell.

vCloud Director creates a task object to track and manage each asynchronous operation that a user requests. Information about all running and recently completed tasks is stored in the vCloud Director database. Because a database upgrade invalidates this task information, you must be sure that no tasks are running when you begin the upgrade process.

With the cell management tool, you can suspend the task scheduler so that new tasks cannot be started, then check the status of all active tasks. You can wait for running tasks to finish or log in to vCloud Director as a system administrator and cancel them. See the Cell Management Tool Reference in the *vCloud Director Administrator's Guide*. When no tasks are running, you can use the cell management tool to stop vCloud Director services.

Prerequisites

- Verify that you have superuser credentials for the target server.
- Verify that you have vCloud Director system administrator credentials.
- If this cell will be accessible to vCloud Director clients while it is being upgraded, use the `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` command to turn on the cell maintenance message.

  ```
  [root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
  ```

  This command causes the cell to respond to all requests with a maintenance message. If you use a load balancer or similar tool to make the cell inaccessible during the upgrade, you do not need to turn on the cell maintenance message.

Procedure

1 Log in to the target server as root.

2 Use the cell management tool to gracefully shut down the cell.

a Retrieve the current job status.

The following `cell-management-tool` command supplies system administrator credentials and returns the count of running jobs.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3
Is Active = true
```

b Stop the task scheduler to quiesce the cell.

Use a `cell-management-tool` command of the following form.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --quiesce true
```

This command prevents new jobs from being started. Existing jobs continue to run until they finish or are cancelled. To cancel a job, use the vCloud Director Web Console or the REST API.

c When the `Job count` value is `0` and the `Is Active` value is `false`, it is safe to shut down the cell.

Use a `cell-management-tool` command of the following form.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --shutdown
```

NOTE You can supply the vCloud Director system administrator password on the `cell-management-tool` command line, but it is more secure to omit the password. This causes the `cell-management-tool` to prompt for the password, which it does not display on the screen as you type.

Console sessions routed through a server's console proxy are interrupted when the server shuts down. If other members of the server group are still active, clients can refresh the console window to recover.

What to do next

After the cell management tool stops vCloud Director services on this server, you can upgrade the server's vCloud Director software or complete other maintenance that the server requires.

Upgrade vCloud Director Software on Any Member of a Server Group

The vCloud Director installer verifies that the target server meets all upgrade prerequisites and upgrades the vCloud Director software on the server.

vCloud Director software is distributed as a digitally signed Linux executable file with a name of the form `vmware-vcloud-director-distribution-`*v.v.v*`-`*nnnnnn*`.bin`, where *v.v.v* represents the product version and *nnnnnn* the build number. For example: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Running this executable installs or upgrades vCloud Director.

IMPORTANT After you upgrade the first member of a server group, you must run a tool that upgrades the group's vCloud Director database before you restart vCloud Director services on the upgraded server. After the database has been upgraded, you can upgrade and re-start other members of the server group.

Prerequisites

- Verify that you have superuser credentials for the target server.

- To have the installer verify the digital signature of the installation file, download and install the VMware public key on the target server. If you already verified the digital signature of the installation file, you do not need to verify it again during installation. See "Download and Install the VMware Public Key," on page 22.
- Use the cell management tool to quiesce and shut down vCloud Director services on the server's cell.
- Verify that you have a valid license key to use the version of the vCloud Director software to which you are upgrading.

Procedure

1 Log in to the target server as root.

2 Download the installation file to the target server.

If you purchased the software on a CD or other media, copy the installation file to a location that is accessible to all target servers.

3 Verify that the checksum of the download matches the one posted on the download page.

Values for MD5 and SHA1 checksums are posted on the download page. Use the appropriate tool to verify that the checksum of the downloaded installation file matches the one shown on the download page. A Linux command of the following form displays the checksum for *installation-file*.

```
[root@cell1 /tmp]# md5sum installation-file
checksum-value installation-file
```

Compare the *checksum-value* produced by this command with the MD5 checksum copied from the download page.

4 Ensure that the installation file is executable.

The installation file requires execute permission. To be sure that it has this permission, open a console, shell, or terminal window and run the following Linux command, where *installation-file* is the full pathname to the vCloud Director installation file.

```
[root@cell1 /tmp]# chmod u+x installation-file
```

5 Use the cell management tool to quiesce the cell and shut down vCloud Director services on the server.

See "Use the Cell Management Tool to Quiesce and Shut Down a Server," on page 41.

6 In a console, shell, or terminal window, run the installation file.

To run the installation file, type its full pathname, for example `./installation-file`. The file includes an installation script and an embedded RPM package.

NOTE You cannot run the installation file from a directory whose pathname includes any embedded space characters.

If the installer detects a version of vCloud Director installed on this server that is equal to or later than the version in the installation file, it displays an error message and exits. Otherwise, it prompts you to confirm that you are ready to proceed to upgrade this server.

```
Checking architecture...done
Checking for a supported Linux distribution...done
Checking for necessary RPM prerequisites...done
Checking free disk space...done
An older version of VMware vCloud Director has been detected
```

7 Respond to the upgrade prompt.

Option	Action
Continue the upgrade.	Type **y**.
Exit to the shell without making any changes in the current installation.	Type **n**.

After you confirm that you are ready to upgrade the server, the installer verifies that the host meets all requirements, unpacks the vCloud Director RPM package, stops vCloud Director services on the server, and upgrades the installed vCloud Director software.

```
Do you wish to proceed with the upgrade? (y/n)? y
Extracting vmware-vcloud-director ......done
Upgrading VMware vCloud Director...
Installing the VMware vCloud Director
Preparing...                ##################################################
vmware-vcloud-director      ##################################################
Migrating settings and files from previous release...done
Migrating in-progress file transfers to /opt/vmware/vcloud-director/data/transfer...done
Uninstalling previous release...done
```

The installer displays a warning of the following form if you did not install the VMware public key on the target server.

```
warning:installation-file.rpm: Header V3 RSA/SHA1 signature: NOKEY, key ID 66fd4949
```

The installer displays a warning of the following form when it makes changes to the existing `global.properties` file on the target server.

```
warning: /opt/vmware/vcloud-director/etc/global.properties created as /opt/vmware/vcloud-director/etc/global.properties.rpmnew
```

Most upgrades require this sort of change, and display this warning. If you have made any changes to the existing `global.properties` file, you can retrieve them from `global.properties.rpmnew`.

8 (Optional) Update logging properties.

After an upgrade, new logging properties are written to the file `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew`.

Option	Action
If you did not change existing logging properties	Copy this file to `/opt/vmware/vcloud-director/etc/log4j.properties`.
If you changed logging properties	Merge `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` file with the existing `/opt/vmware/vcloud-director/etc/log4j.properties`. Merging these files preserves your changes.

When the vCloud Director software upgrade is complete, the installer displays a message indicating where the old configuration files are stored, then reminds you to run the database upgrade tool.

What to do next

- If you have not already done so, upgrade the vCloud Director database that this server uses.
- If you already upgraded the vCloud Director database that this server group uses, you can restart the upgraded server. See "Start or Stop vCloud Director Services," on page 36.

Upgrade the vCloud Director Database

After you upgrade a server in your vCloud Director server group, you must upgrade the group's vCloud Director database before you restart vCloud Director services on the server.

All servers in a vCloud Director server group share the same database, so regardless of how many servers you are upgrading, you need to upgrade the database only once. After the database is upgraded, vCloud Director servers cannot connect to it until they, too, are upgraded.

Prerequisites

IMPORTANT Back up your existing database before you upgrade it. Use the procedures that your database software vendor recommends.

Verify that all vCloud Director cells are inactive. See "Use the Cell Management Tool to Quiesce and Shut Down a Server," on page 41

Procedure

1 Open a console, shell, or terminal window, and type the following command to run the database upgrade script.

```
/opt/vmware/vcloud-director/bin/upgrade
```

IMPORTANT If the database upgrade script detects that an incompatible version of vShield Manager or NSX Manager is registered to this installation of vCloud Director, it displays a warning message and cancels the upgrade.

```
One or more vShield Manager servers registered to this vCloud
Director installation are not supported by the version of vCloud Director
you are upgrading to. Upgrade canceled, please follow the procedures in
the vShield Manager Upgrade Guide to upgrade those unsupported vShield
Manager servers.
```

2 Respond to the database upgrade prompts.

a Confirm that you want to continue with the database upgrade.

```
Welcome to the vCloud Director upgrade utility

Verify that you have a valid license key to use the version of
the vCloud Director software to which you are upgrading.

This utility will apply several updates to the database. Please
ensure you have created a backup of your database prior to continuing.

Do you wish to upgrade the product now? [Y/N]:
```

Take one of the following actions:

Option	Action
Continue the upgrade.	Type **y**.
Exit to the shell without making any changes in the current vCloud Director database.	Type **n**.

b (Optional) Wait for cells to become inactive, if necessary.

If the database upgrade tool detects that any cells are still active, it prompts you to continue with the upgrade or exit.

```
Found active cell. Name: "cell-01", IP Address: 10.150.151.190, Identifier: a2eb...
Do you wish to upgrade the database while cells are still active? [Y/N]
```

If you see this prompt, type `n` to exit to the shell, then wait five minutes and restart the database upgrade tool. If the database upgrade tool continues to warn you about cells that are still active, return to the procedure in "Use the Cell Management Tool to Quiesce and Shut Down a Server," on page 41 and ensure that all cells have become inactive.

After you have responded to all prompts, the database upgrade tool runs and displays progress messages.

```
Executing upgrade task: Start UpdateStatementManager
...[3]
Successfully ran upgrade task
Executing upgrade task: ...
.......... Successfully ran upgrade task
...
Executing upgrade task: Stop UpdateStatementManager
...[3]
...
Successfully ran upgrade task
```

After the database is upgraded, the upgrade script offers to start vCloud Director services on this host.

```
Would you like to start the vCloud Director service now? If you choose not
to start it now, you can manually start it at any time using this command:
    service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment).
Starting vmware-vcd-watchdog:                              [  OK  ]
Starting vmware-vcd-cell                                   [  OK  ]
```

Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System

Before you upgrade a vCenter Server system and hosts attached to vCloud Director, you must upgrade each NSX Manager that is associated with that vCenter Server system.

Upgrading NSX Manager interrupts access to NSX administrative functions but does not interrupt network services.

IMPORTANT Verify that at least one cell in your vCloud Director installation is upgraded and running before you begin the NSX upgrade. If no cell is running, data about the upgraded NSX Manager cannot be written to the vCloud Director database.

Prerequisites

- Upgrade at least one vCloud Director cell.
- Upgrade the vCloud Director database.

Procedure

- Upgrade the NSX Manager associated with each vCenter Server systems registered to your vCloud Director installation.

  For information about upgrading NSX, see the NSX for vSphere Documentation Center at https://www.vmware.com/support/pubs/nsx_pubs.html.

After the upgrade finishes, the upgraded NSX Manager notifies vCloud Director that the software is at a new version. It can take several minutes before the notification is sent and vCloud Director processes it.

What to do next

After you have upgraded all your NSX Managers, you can upgrade your registered vCenter Server systems and ESXi hosts.

Upgrade vCenter Server Systems, Hosts, and NSX Edges

After you have upgraded vCloud Director and NSX Manager, you must upgrade the vCenter Server systems and ESXi hosts attached to your cloud. After all of the attached vCenter Server systems and hosts are upgraded, you can upgrade the NSX Edges.

Prerequisites

Verify that you have already upgraded each NSX Manager that is associated with the vCenter Server systems that are attached to your cloud. See "Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System," on page 47.

Procedure

1. Upgrade the attached vCenter Server system.

   See the *vSphere Installation and Setup Guide*.

2. Verify all vCloud Director public URLs and certificate chains.

   On the **Administration** tab of the vCloud Director Web console, click **Public Addresses** in the left pane. Enter values for all fields.

3 (Optional) If you have configured vCloud Director to use vCenter Single Sign On, you must unregister and re-register vCloud Director with the vCenter Lookup Service.

   a Log in to vCloud Director as a system administrator using a local or LDAP account. Do not use vCenter Single Sign On for this log in.

   b Unregister vCloud Director with the vCenter Lookup Service.

   On the **Administration** tab of the vCloud Director Web console, click **Federation** in the left pane, and click **Unregister**. You must provide the appropriate vCenter administrator credentials to complete this action.

   c Register vCloud Director with the vCenter Lookup Service.

   See "Configure vCloud Director to use vCenter Single Sign On" in the*vCloud Director Administrator's Guide*

4 Refresh the vCenter Server system's registration with vCloud Director.

   a In the vCloud Director Web console, click the **Manage & Monitor** tab and click **vCenters** in the left pane.

   b Right-click the vCenter Server name and select **Refresh**.

   c Click **Yes**.

5 Upgrade each ESXi host that the upgraded vCenter Server system supports.

   See the *vSphere Installation and Setup Guide*. For each host, the upgrade requires the following steps:

   a In the vCloud Director Web console, disable the host.

   On the **Manage and Monitor** page, click **Hosts**, then right-click the host and select **Disable Host**.

   b Use the vCenter Server system to put the host into maintenance mode and allow all the virtual machines on that host to migrate to another host.

   c Upgrade the host.

   To ensure that you have enough upgraded host capacity to support the virtual machines in your cloud, upgrade hosts in small batches. When you do this, host agent upgrades can complete in time to allow virtual machines to migrate back to the upgraded host.

   d Use the vCenter Server system to reconnect the host.

   e Upgrade the vCloud Director host agent on the host.

   See "Upgrade an ESX/ESXi Host Agent" in the *vCloud Director Administrator's Guide*.

   f In the vCloud Director Web console, enable the host.

   On the **Manage and Monitor** page, click **Hosts**, then right-click the host and select **Enable Host**.

   g Use the vCenter Server system to take the host out of maintenance mode.

6 (Optional) Upgrade NSX Edges managed by the NSX Manager associated with the upgraded vCenter Server system.

   Upgraded NSX Edges deliver improvements in performance and integration. You can use either NSX Manager or vCloud Director upgrade NSX Edges.

   - For information about using NSX Manager to upgrade NSX Edges, see the NSX for vSphere Documentation Center at https://www.vmware.com/support/pubs/nsx_pubs.html.
   - To use vCloud Director to upgrade an NSX Edges, you must operate on the vCloud Director network object that the Edge supports:
     - An appropriate upgrade of an Edge Gateway occurs automatically when you use either the vCloud Director Web console or REST API to reset a network that the Edge Gateway serves.

- Redeploying an Edge Gateway upgrades the associated NSX Edge appliance.
- Resetting a vApp network from within the context of the vApp upgrades the NSX Edge appliance associated with that network. To use vCloud Director Web console to reset a vApp network from within the context of a vApp, navigate to the **Networking** tab for the vApp, display its networking details, right-click the vApp network, and select **Reset Network**.

For more information on how to redeploy edge gateways and reset vApp networks, see the vCloud Director Web console online help or the *vCloud API Programming Guide*.

IMPORTANT Regardless of whether you use NSX Manager or vCloud Director to upgrade your Edges, at least one vCloud Director cell must upgraded and running before you begin the upgrade. If no cell is running, data about the upgraded NSX Edges cannot be written to the vCloud Director database.

What to do next

Repeat this procedure for the other vCenter Server systems registered to your vCloud Director installation.

vCloud Director Setup 4

After you configure all servers in the vCloud Director server group and connect them to the database, you can initialize the server group's database with a license key, system administrator account, and related information. When this process is complete, you can use the vCloud Director Web Console to complete the initial provisioning of your cloud.

Before you can run the vCloud Director Web Console, you must run the Setup wizard, which gathers the information that the Web Console requires before it can start. After the wizard is finished, the Web Console starts and displays the login screen. The vCloud Director Web Console provides a set of tools for provisioning and managing a cloud. It includes a Quickstart feature that guides you through steps like attaching vCloud Director to vCenter and creating an organization.

As an alternative to using the Setup wizard, you can use command-line tools to configure the system. See the Cell Management Tool Reference in the *vCloud Director Administrator's Guide*.

Prerequisites

- Complete the installation of all vCloud Director servers, and verify that vCloud Director services have started on all servers.
- Verify that you have the URL that the configuration script displays when it completes.

> **NOTE** To discover the URL of the Setup wizard after the script exits, look up the fully qualified domain name associated with the IP address you specified for the HTTP service during installation of the first server and use it to construct a URL of the form https://*fully-qualified-domain-name*, for example, https://mycloud.example.com. You can connect to the wizard at that URL.

Complete the installation of all vCloud Director servers, and verify that vCloud Director services have started on all servers.

Procedure

1 Open a Web browser and connect to the URL that the configuration script displays when it completes.

> **NOTE** You might have to wait a few minutes after starting vCloud Director services for the Setup wizard or Web console to become ready.

2 Follow the prompts to complete the setup.

This chapter includes the following topics:

- "Ready to Log In to vCloud Director," on page 53

Review the License Agreement

Before you can configure a vCloud Director server group, you must review and accept the end user license agreement.

Procedure

1 Review the license agreement.

2 Accept or reject the agreement.

Option	Action
To accept the license agreement.	Click **Yes, I accept the terms in the license agreement**.
To reject the license agreement	**No, I do not accept the terms in the license agreement**.

If you reject the license agreement, you cannot proceed with vCloud Director configuration.

Enter the License Key

Each vCloud Director cluster requires a license to run. The license is specified as a product serial number. The product serial number is stored in the vCloud Director database.

The vCloud Director product serial number is not the same as the vCenter server license key. To operate a vCloud, you must have a vCloud Director product serial number and a vCenter server license key. You can obtain both types of license keys from the VMware License Portal.

Procedure

1 Obtain a vCloud Director product serial number from the VMware License Portal.

2 Type the product serial number in the **Product serial number** text box.

Create the System Administrator Account

Specify the user name, password, and contact information for the vCloud Director system administrator.

The vCloud Director system administrator has superuser privileges throughout the cloud. You create the initial system administrator account during vCloud Director setup. After installation and configuration is complete, this system administrator can create additional system administrator accounts as needed.

Procedure

1 Type the system administrator's user name.

2 Type the system administrator's password and confirm it.

3 Type the system administrator's full name.

4 Type the system administrator's email address.

Specify System Settings

You can specify the system settings that control how vCloud Director interacts with vSphere and NSX Manager.

The configuration process creates a folder in the attached vCenter Server system for vCloud Director to use and specifies an installation ID to use when you create MAC addresses for virtual NICs.

Procedure

1 Type a name for the vCloud Director vCenter Server folder in the **System name** field.

2 Use the **Installation ID** field to specify the installation ID for this installation of vCloud Director.

If a datacenter includes multiple installations of vCloud Director, each installation must specify a unique installation ID.

Ready to Log In to vCloud Director

After you provide all of the information that the Setup Wizard requires, you can confirm your settings and complete the wizard. After the wizard finishes, the login screen of the vCloud Director Web Console appears.

The Ready to Log In page lists all the settings you have provided to the wizard. Review the settings carefully.

Prerequisites

Verify that you have access to the vCenter Server system initially registered to your installation, and to that vCenter Server system's associated NSX Manager. The vCloud Director Web Console requires access to the installations of vCenter Server and NSX Manager that you want to configure as part of this vCloud Director installation. These installations must be running and configured to work with each other before you finish this task. For more information about the configuration requirements, see "vCloud Director Hardware and Software Requirements," on page 9.

Procedure

- To change a setting, click **Back** until you get to the page where the setting originated.
- To confirm all settings and complete the configuration process, click **Finish**.

When you click **Finish**, the wizard applies the settings you specified, then starts the vCloud Director Web Console and displays its login screen.

What to do next

Use the displayed login screen to log in to the vCloud Director Web Console using the user name and password you provided for the system administrator account. After you have logged in, the console displays a set of Quickstart steps that you must complete before you can use this cloud. When the steps are complete, the Guided Tasks are enabled, and your cloud is ready for use.

Install and Configure Optional Database Software to Store and Retrieve Historic Virtual Machine Performance Metrics

5

vCloud Director can collect metrics that provide current and historic information about virtual machine performance and resource consumption for the virtual machines that are in your cloud. Data for historic metrics is stored in a KairosDB database backed by a Cassandra cluster.

Cassandra and KairosDB are open source databases that, when deployed together, provide a scalable, high-performance solution for collecting time series data like virtual machine metrics. If you want your cloud to support retrieval of historic metrics from virtual machines, you must install and configure Cassandra and KairosDB, then use the `cell-management-tool` utility to connect vCloud Director to KairosDB. Retrieval of current metrics does not require optional database software.

To support retrieval of historic metrics, vCloud Director requires a Cassandra cluster. A Cassandra cluster consists of one or more machines on which you have installed Cassandra and are running the Cassandra service. For a typical vCloud Director installation, you should have at least three machines in the Cassandra cluster. Because the vCloud Director metrics monitoring feature uses a replication factor of two, having three machines, the nodes, in the Cassandra cluster ensures that a node is always available to handle a transaction. You can use a single Cassandra cluster for your vCloud Director installation.

You also need at least one instance of KairosDB configured to work with your Cassandra cluster. If your cloud collects historic metrics from many virtual machines, additional instances of KairosDB might be needed. You can either install and configure KairosDB on one of the Cassandra nodes and point the cell management tool to that endpoint, or install and configure KairosDB on each Cassandra node, add a load balancer in front of the configuration, and point the cell management tool at the load balancer endpoint. Because vCloud Director expects to communicate with KairosDB at a single IP address, installations that include multiple instances of KairosDB must use a load balancer to provide that address and distribute vCloud Director requests to the KairosDB instances.

Prerequisites

- Verify that vCloud Director is installed and running before you configure the optional database software.
- If you are not already familiar with Cassandra and KairosDB, review the material available at http://cassandra.apache.org/ and https://code.google.com/p/kairosdb/.
- Obtain either Cassandra 1.2.*x* or Cassandra 2.0.*x* from http://cassandra.apache.org/download/.
- Obtain KairosDB 0.9.1 from https://code.google.com/p/kairosdb/.
- Complete the installation and configuration of the Cassandra cluster that you plan to use with your vCloud Director installation, according to this configuration:
  - Cassandra 1.2.*x* or Cassandra 2.0.*x* is installed on at least three machines that are connected to the same network that your vCloud Director cells use.
  - The machines are configured to have their own physical storage, and not shared storage.

  - The machines are configured as a Cassandra cluster.
  - Java Native Access (JNA) version 3.2.7 or later is enabled for the Cassandra cluster, to improve performance of memory usage and disk access.
- Complete the installation and configuration of at least one instance of KairosDB 0.9.1 on one of the Cassandra nodes, to use your Cassandra cluster as its database. You can also install and configure KairosDB on each Cassandra node if you add a load balancer in front of that configuration.
- Verify that KairosDB and Cassandra are configured correctly. Use a Web browser to browse to `http://KairosDB-IP:8080/api/v1/metricnames`. If the page opens without an error, KairosDB and Cassandra are configured correctly.
- Verify that you can run the `service` command of the `cell-management-tool` utility. For details about the `service` command, see "Start or Stop vCloud Director Services," on page 36.

Procedure

1 Use the `cell-management-tool` utility to configure a connection between vCloud Director and KairosDB.

  Use a command like this, where *KairosDB-IP* is the IP address of the machine on which you installed KairosDB, or the IP address of the load balancer you are using to distribute requests to multiple instances of KairosDB.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics
  --repository-host KairosDB-IP --repository-port 8080
```

2 Restart each vCloud Director cell using the `service` command of the `cell-management-tool` utility.

Index