vCloud Director Installation and Upgrade Guide

04 OCT 2018

vCloud Director 9.5

vmware®

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

https://docs.vmware.com/

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 5

Updated Information 6

1 Overview of vCloud Director Installation, Configuration, and Upgrade 7
- vCloud Director Architecture 7
- Configuration Planning 8

2 vCloud Director Hardware and Software Requirements 9
- Network Configuration Requirements for vCloud Director 10
- Network Security Requirements 11

3 Before You Install vCloud Director or Deploy the vCloud Director Appliance 14
- Preparing the vCloud Director Database 14
- Preparing the Transfer Server Storage 17
- Install and Configure a RabbitMQ AMQP Broker 18
- Create SSL Certificates 19
- Download and Install the VMware Public Key 27
- Install and Configure NSX Data Center for vSphere for vCloud Director 27
- Install and Configure NSX-T Data Center for vCloud Director 28

4 Install vCloud Director on Linux 30
- Install vCloud Director on the First Member of a Server Group 31
- Configure the Network and Database Connections 33
- Install vCloud Director on an Additional Member of a Server Group 40
- Set Up vCloud Director 42

5 Deploy the vCloud Director Appliance 44
- Start the vCloud Director Appliance Deployment 45
- Customize the vCloud Director Appliance and Finish the Deployment 45

6 After you Install vCloud Director or Deploy the vCloud Director Appliance 48
- Perform Additional Configurations on the PostgreSQL Database 48
- Customize Public Endpoints 50
- Install Microsoft Sysprep Files on the Servers 52
- Install and Configure a Cassandra Database for Storing Historic Metric Data 54
- Editing the DNS Settings of the vCloud Director Appliance 55

7 Upgrading vCloud Director 56

Perform an Orchestrated Upgrade of a vCloud Director Installation 57

Manually Upgrade a vCloud Director Installation 60

Database Upgrade Utility Reference 65

8 After you Upgrade vCloud Director 68

Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System 68

Upgrade vCenter Server Systems, ESXi Hosts, and NSX Edges 69

Rights and Roles After the Upgrade 70

9 Uninstall vCloud Director Software 72

vCloud Director Installation and Upgrade Guide

The *vCloud Director Installation and Upgrade Guide* provides information about installing and upgrading VMware vCloud Director® for Service Providers software and configuring it to work with VMware vSphere®, VMware NSX® for vSphere®, and VMware NSX-T™ Data Center.

Intended Audience

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

Updated Information

This *vCloud Director Installation and Upgrade Guide* is updated with each release of the product or when necessary.

This table provides the update history of the *vCloud Director Installation and Upgrade Guide*.

Revision	Description
01 FEB 2019	■ Updated Configure a PostgreSQL Database to add a step for creating the database user. ■ Updated Network Configuration Requirements for vCloud Director to add the information that the vCloud Director appliance uses a single IP address with custom port 8443 for the console proxy service. ■ Updated Step 8 in Install vCloud Director on an Additional Member of a Server Group to add the command for the case when the console proxy service uses a custom port. ■ Updated and added topic Customize Public Endpoints, which contains postrequisite information after deploying the vCloud Director appliance.
15 JAN 2019	Updated chapter Chapter 7 Upgrading vCloud Director to correct the workflow for upgrading a vCloud Director installation with an Oracle database.
09 JAN 2019	Added topic Editing the DNS Settings of the vCloud Director Appliance.
17 DEC 2018	Updated Chapter 4 Install vCloud Director on Linux and Chapter 5 Deploy the vCloud Director Appliance to state that mixed vCloud Director installations on Linux and vCloud Director appliances in one server group is unsupported.
30 NOV 2018	Updated Chapter 7 Upgrading vCloud Director to add the vCloud Director appliance to the upgrade procedures.
09 NOV 2018	Updated Chapter 5 Deploy the vCloud Director Appliance to add an Important note and restructure the information.
26 OCT 2018	■ Updated Chapter 5 Deploy the vCloud Director Appliance to state that deploying the vCloud Director appliance from the vSphere Client is unsupported. ■ Updated Rights and Roles After the Upgrade to state that before starting to use the rights bundles model for an existing organization, you must delete the corresponding Legacy Rights Bundle.
04 OCT 2018	Initial release.

Overview of vCloud Director Installation, Configuration, and Upgrade

1

You create a vCloud Director server group by installing the vCloud Director software on one or more Linux servers, or by deploying one or more instances of the vCloud Director appliance. During the installation process, you perform the initial vCloud Director configuration, which includes establishing network and database connections.

After you create the vCloud Director server group, you integrate the vCloud Director installation with your vSphere resources. For network resources, vCloud Director can use NSX Data Center for vSphere, NSX-T Data Center, or both.

When you upgrade an existing vCloud Director installation, you update the vCloud Director software and the database schema, leaving the existing relationships between servers, the database, and vSphere in place.

This chapter includes the following topics:

- vCloud Director Architecture
- Configuration Planning

vCloud Director Architecture

A vCloud Director server group consists of one or more Linux servers. Each server in the group runs a collection of services called a vCloud Director cell. All cells share a single vCloud Director database and a transfer server storage, and connect to the vSphere and network resources.

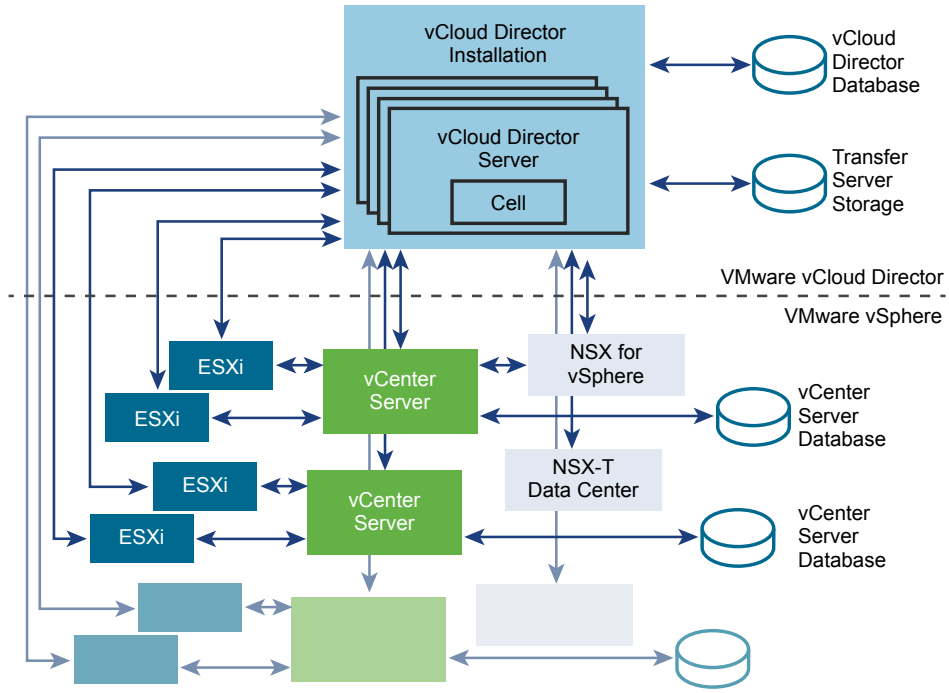
To ensure vCloud Director high availability, you must install at least two vCloud Director cells in a server group. When you use a third-party load balancer, you can ensure an automatic failover without downtime.

A typical installation creates a vCloud Director server group comprising several servers. You can install vCloud Director for Linux on each server or deploy one or more instances of the vCloud Director appliance.

Important Mixed vCloud Director Linux installations and vCloud Director appliances are unsupported.

You can connect a vCloud Director installation to multiple VMware vCenter Server® systems and the VMware ESXi™ hosts that they manage. For network services, vCloud Director can use NSX Data Center for vSphere associated with vCenter Server or you can register NSX-T Data Center with vCloud Director. Mixed NSX Data Center for vSphere and NSX-T Data Center are also supported.

Figure 1-1. vCloud Director Architecture Diagram



The vCloud Director installation and configuration process creates the cells, connects them to the shared database and transfer server storage, and creates the system administrator account. Then the system administrator establishes connections to the vCenter Server system, the ESXi hosts, and the NSX Manager instances. For information about adding vSphere and network resources, see the *vCloud Director Administrator's Guide*.

Configuration Planning

vSphere provides storage, compute, and networking capacity to vCloud Director. Before you begin installation, consider how much vSphere and vCloud Director capacity your cloud requires, 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 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 Chapter 2 vCloud Director Hardware and Software Requirements.
- Configure the vCloud Director database as described in Preparing the vCloud Director Database.

vCloud Director Hardware and Software Requirements 2

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 system, an NSX Manager instance, 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

vCenter Server instances and ESXi hosts intended for use with vCloud Director must meet specific configuration requirements.

- vCenter Server 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 data center simplifies the task of adding new vCenter Server instances to vCloud Director.
- vSphere Distributed Switches are required for isolated networks and network pools backed by NSX Data Center for vSphere.
- vCenter Server 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 Server instances 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.

Disk Space, Memory, and CPU Requirements

Physical requirements such as disk space, memory, and CPU for vCloud Director cells are listed in the *vCloud Director Release Notes*.

Shared Storage

NFS or other shared storage volume for the vCloud Director transfer service. The storage volume must be expandable and accessible to all servers in the server group.

This chapter includes the following topics:

- Network Configuration Requirements for vCloud Director
- Network Security Requirements

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 host names, a network time service, and other services. Your network must meet these requirements before you begin installing vCloud Director.

The network that connects the vCloud Director servers, the database server, the vCenter Server systems, and the NSX 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 endpoint 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. Do not use the Linux `ip addr add` command to create the second address.

The vCloud Director appliance uses a single IP address with custom port 8443 for the console proxy service.

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.

For an installation with a single IP address, you can customize the console proxy address from the vCloud Director Web Console. For example, for the vCloud Director appliance, you must customize the console proxy address to *vcloud.example.com*:8443.

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.

Host Name 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
```

Network Security Requirements

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, including requests to JMX (port 8999) must be rejected by the firewall.

Table 2-1. 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

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

Port	Protocol	Comments
61611	TCP	AMQP
61616	TCP	AMQP

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

Table 2-2. 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 using the standard port. If you have chosen a different port for these services, disable connection to port 443 and enable them for the port you have chosen.
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.
5672	TCP, UDP	Optional. AMQP messages for task extensions.
61611	TCP	AMQP
61616	TCP	AMQP

- Route traffic between vCloud Director servers and the following servers over a dedicated private network.
  - vCloud Director database server
  - RabbitMQ
  - Cassandra
- If possible, route traffic between vCloud Director servers, vSphere, and NSX over a dedicated private network.
- Virtual switches and distributed virtual switches that support provider networks must be isolated from each other. They cannot share the same layer 2 physical network segment.

- Use NFSv4 for transfer service storage. The most common NFS version, NFSv3, does not offer on transit encryption which in some configurations might enable in-flight sniffing or tampering with data being transferred. Threats inherent in NFSv3 are described in the SANS white paper NFS Security in Both Trusted and Untrusted Environments. Additional information about configuring and securing the vCloud Director transfer service is available lin VMware Knowledge Base article 2086127.

Before You Install vCloud Director or Deploy the vCloud Director Appliance

3

Before you install vCloud Director on a Linux server or deploy the vCloud Director appliance, you must prepare your environment.

This chapter includes the following topics:

- Preparing the vCloud Director Database
- Preparing the Transfer Server Storage
- Install and Configure a RabbitMQ AMQP Broker
- Create SSL Certificates
- Download and Install the VMware Public Key
- Install and Configure NSX Data Center for vSphere for vCloud Director
- Install and Configure NSX-T Data Center for vCloud Director

Preparing the vCloud Director Database

The vCloud Director cells use a database to store shared information. You must install and configure the vCloud Director database before you create the vCloud Director server group.

For information about the supported vCloud Director databases, see the VMware Product Interoperability Matrixes.

Regardless of the database software you decide to use, 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.

Important vCloud Director supports SSL connections only to a PostgreSQL database. You can enable SSL on the PostgreSQL database during an unattended network and database connections configuration or after creating the vCloud Director server group. See Unattended Configuration Reference and Perform Additional Configurations on the PostgreSQL Database.

Configure a PostgreSQL Database

PostgreSQL databases have specific configuration requirements when you use them with vCloud Director. Before you install vCloud Director, you must install and configure a database instance and create the vCloud Director database user account.

Prerequisites

You must be familiar with PostgreSQL commands, scripting, and operation.

Procedure

1 Configure the database server.

   A database server with 16 GB of memory, 100 GB storage, and 4 CPUs is appropriate for typical vCloud Director server groups.

2 Install a supported distribution of PostgreSQL on the database server.

   - The `SERVER_ENCODING` value of the database must be `UTF-8`. This value is established when you install the database and always matches the encoding used by the database server operating system.
   - Use the PostgreSQL `initdb` command to set the value of `LC_COLLATE` and `LC_CTYPE` to `en_US.UTF-8`. For example:

     ```
     initdb --locale=en_US.UTF-8
     ```

3 Create the database user.

   The following command creates the user `vcloud`.

   ```
   create user vcloud;
   ```

4 Create the database instance and give it an owner.

   Use a command like this one to specify a database user named `vcloud` as the database owner.

   ```
   create database vcloud owner vcloud;
   ```

5 Assign a database password to the database owner account.

   The following command assigns the password `vcloudpass` to database owner `vcloud`.

   ```
   alter user vcloud password 'vcloudpass';
   ```

6 Enable the database owner to log in to the database.

   The following command assigns the `login` option to database owner `vcloud`.

   ```
   alter role vcloud with login;
   ```

What to do next

After creating your vCloud Director server group, you can configure the PostgreSQL database to require SSL connections from the vCloud Director cells and adjust some database parameters for optimal performance. See Perform Additional Configurations on the PostgreSQL Database.

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.
- See VMware Knowledge Base article https://kb.vmware.com/kb/2148767 for information about using Microsoft SQL Server Always On Availability Groups with the vCloud Director database.

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 server groups.

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
```

Preparing the 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.

Important The vCloud Director appliance supports only NFS type of shared storage. The appliance deployment process involves mounting the NFS shared transfer server storage.

When NFS is used for the transfer server storage, you must configure each vCloud Director cell in the vCloud Director server group to mount and use the NFS-based transfer server storage. See http://kb.vmware.com/kb/2086127.

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:

- During transfers, uploads and downloads occupy this storage. When the transfer finishes, the uploads and downloads are removed from the storage. 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 the published content occupy this storage. 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, you can assume that hundreds or even thousands of catalog items require space on this volume. The size of each catalog item is about the size of a virtual machine in a compressed OVF form.

Note The volume of the transfer server storage must be easily expanded.

Install and Configure a RabbitMQ AMQP Broker

AMQP, the Advanced Message Queuing Protocol, is an open standard for message queuing that supports flexible messaging for enterprise systems. vCloud Director uses the RabbitMQ AMQP broker to provide the message bus used by extension services, object extensions, and notifications.

Procedure

1. Download the RabbitMQ Server from https://www.rabbitmq.com/download.html.

   See the *vCloud Director Release Notes* for the list of supported RabbitMQ releases.
2. Follow the RabbitMQ installation instructions and install RabbitMQ on a supported 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 are required for 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 user name 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. You can configure the AMQP service to encrypt these messages by using SSL. You can also configure the service to verify the broker certificate by using the default JCEKS trust store of the Java runtime environment on the vCloud Director cell, typically at `$VCLOUD_HOME/jre/lib/security/cacerts`.

To enable SSL with the vCloud Director AMQP service:

1 In the vCloud Director Web console, click the **Administration** tab, and click **Extensibility**.

2 Click **Extensibility**, and click the **Settings** tab.

3 In the **AMQP Broker Settings** section, select **Use SSL**.

4 Either select the **Accept all certificates** check box or provide one of the following:

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

Create SSL Certificates

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

Note This procedure is required only for installing vCloud Director on Linux. The vCloud Director appliance first boot creates a self-signed SSL certificate. After the appliance deployment, you can Create and Import a Signed SSL Certificate.

Each vCloud Director server must support two different SSL endpoints. These endpoints can be separate IP addresses, 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 and the fully qualified domain name associated with it. Decide which IP address is for the HTTP service and which IP address is for the console proxy service.

You must provide the fully qualified domain names when you create the certificates, and the IP addresses when you configure the network and database connections. If any, make a note of other fully qualified domain names that can reach the IP address, because you must provide 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.

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.
- 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 3-1. 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:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

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 –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

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 –ext "san=dns:vcd2.example.com,dns:vcd2,ip:
10.100.101.10"
```

5 Send the certificate signing requests to your Certificate 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 Certificate 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 the Network and Database Connections.

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.

You can generate self-signed certificates for the cell manually using this procedure, or you can use the `generate-certs` command of the cell management tool to generate new self-signed SSL certificates for the cell, as shown in Example: Using the Cell Management Tool to Create Self-Signed Certificates. For more information, see "Generating Self-Signed SSL Certificates" in the *vCloud Director Administrator's Guide*.

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.

Prerequisites

You can generate self-signed certificates for the cell manually using this procedure, or you can use the `generate-certs` command of the cell management tool to generate new self-signed SSL certificates for the cell. For more information, see "Generating Self-Signed SSL Certificates" in the *vCloud Director Administrator's Guide*.

- 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.
- 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 3-2. 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:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

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.

Example: Using the Cell Management Tool to Create Self-Signed Certificates

The `cell–management–tool` utility is installed on the cell before the configuration agent runs. After you have run the installation file as shown in Install vCloud Director on the First Member of a Server Group, you can use the `cell–management–tool` to create self-signed certificates before you configure the system's network and database connections.

The command shown in this example creates or updates a keystore at `/tmp/cell.ks` that has the password `kspw`. Certificates are created using the command's default values. The issuer name is set to `CN=Unknown`. The certificate uses the default 2048-bit key length and expires one year after creation.

```
[root@cell1 /opt/vmware/vcloud–
director/bin]# ./cell–management–tool generate–certs –j –p –o /tmp/cell.ks –w kspw
New keystore created and written to /tmp/cell.ks.
```

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.

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 the Network and Database Connections.

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.

Install and Configure NSX Data Center for vSphere for vCloud Director

If you plan your vCloud Director installation to use network resources from NSX Data Center for vSphere, you must install and configure NSX Data Center for vSphere and associate a unique NSX Manager instance with each vCenter Server instance that you plan to include in your vCloud Director installation.

NSX Manager is included in the NSX Data Center for vSphere download. For the most recent information about compatibility between vCloud Director and other VMware products, see the *VMware Product Interoperability Matrices* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. For information about the network requirements, see Network Configuration Requirements for vCloud Director.

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 7 Upgrading vCloud Director.

Prerequisites

Verify that each of your vCenter Server systems meets the prerequisites for installing NSX Manager.

Procedure

1. Perform the installation task for the NSX Manager virtual appliance.

   See the *NSX Installation Guide*.

2. Log in to the NSX Manager virtual appliance that you installed and confirm the settings that you specified during installation.
3. 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.
4. Configure VXLAN support in the associated NSX Manager instances.

   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*.

5. (Optional) If you want Edge Gateways in the system to provide distributed routing, set up an NSX Controller cluster.

   See the *NSX Administration Guide*.

Install and Configure NSX-T Data Center for vCloud Director

If you plan your vCloud Director installation to use network resources from NSX-T Data Center, you must install and configure NSX-T Data Center with at least one NSX-T Manager instance.

NSX-T Manager is included in the NSX-T Data Center download. For the most recent information about compatibility between vCloud Director and other VMware products, see the *VMware Product Interoperability Matrices* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. For information about the network requirements, see Network Configuration Requirements for vCloud Director.

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 7 Upgrading vCloud Director.

Prerequisites

You must be familiar with NSX-T Data Center.

Procedure

1. Install the NSX-T Manager virtual appliance.

   See the *NSX-T Installation Guide*.

2. Prepare the ESXi hosts that you want to operate with NSX-T Data Center.

   See the *NSX-T Installation Guide*.

3. Create transport nodes and transport zones for your cloud requirements.

   See the *NSX-T Installation Guide*.

4. Configure edge nodes and clusters.

   See the *NSX-T Installation Guide*.

5. Configure tier-0 and tier-1 routers.

   See the *NSX-T Administration Guide*.

6. Configure one or more VLAN or overlay logical switches that you want to import to your vCloud Director installation.

   See the *NSX-T Administration Guide*.

What to do next

After you install vCloud Director, you can register the NSX-T Manager instance with your cloud. For information about registering an NSX-T Manager instance, see *vCloud API Programming Guide for Service Providers*.

Install vCloud Director on Linux

4

You can create a vCloud Director server group by installing the vCloud Director software of one or more Linux servers. Installation and configuration of the first group member creates a response file that you use to configure additional members of the group.

This procedure applies to new installations only. If you are upgrading an existing vCloud Director installation, see Chapter 7 Upgrading vCloud Director.

Important Mixed vCloud Director installations on Linux and vCloud Director appliances in one server group are unsupported.

Prerequisites

- Verify that the target servers for your server group meet the Chapter 2 vCloud Director Hardware and Software Requirements.
- Verify that you created an SSL certificate for each endpoint of the target servers for your server group. All directories in the pathname to the SSL certificates must be readable by any user. Using the same keystore path on all members of a server group simplifies the installation process, for example `/tmp/certificates.ks`. See Create SSL Certificates.
- Verify that you prepared an NFS or other shared storage volume that is accessible to all target servers for your vCloud Director server group. See Preparing the Transfer Server Storage.
- Verify that you created a vCloud Director database that is accessible to all servers in the group. See Preparing the vCloud Director Database. Verify that the database service starts when you reboot the database server.
- Verify that all vCloud Director servers, the database server, all vCenter Server systems, and the associated NSX Manager instances can resolve each host name in the environment as described in Network Configuration Requirements for vCloud Director.
- Verify that all vCloud Director servers and the database server are synchronized to a network time server with the tolerances noted in Network Configuration Requirements for vCloud Director.
- If you plan to import users or groups from an LDAP service, verify that the service is accessible to each vCloud Director server.
- Open firewall ports as shown in Network Security Requirements. Port 443 must be open between vCloud Director and vCenter Server systems.

Procedure

1 Install vCloud Director on the First Member of a Server Group

After you prepared your environment and verified the prerequisites, you can begin creating the vCloud Director server group by running the vCloud Director installer on the first target Linux server.

2 Configure the Network and Database Connections

After you install vCloud Director on the first member of the server group, you must run the configuration script that creates the network and database connections for this cell. The script creates a response file that you must use when configuring additional members of the server group.

3 Install vCloud Director on an Additional Member 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.

4 Set Up vCloud Director

After you install and configure all servers in the vCloud Director server group, you must set up your vCloud Director installation. The vCloud Director setup initializes the vCloud Director database with a license key, system administrator account, and related information.

What to do next

You can begin adding resources to your vCloud Director installation. To get started with vCloud Director, see *vCloud Director Administrator's Guide*.

Install vCloud Director on the First Member of a Server Group

After you prepared your environment and verified the prerequisites, you can begin creating the vCloud Director server group by running the vCloud Director installer on the first target Linux server.

vCloud Director for Linux is distributed as a digitally signed 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.

Prerequisites

- Verify that you have superuser credentials for the target server.
- If you want the installer to 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.

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 media, copy the installation file to a location that is accessible to the target server.
3. Verify that the checksum of the download matches the checksum 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 checksum shown on the download page. A Linux command of the following form displays the checksum for *installation-file*.

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

   The command returns the installation file checksum that must match the MD5 checksum 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. Run the installation file.

   To run the installation file, enter the 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.

   If you did not install the VMware public key on the target server, the installer prints a warning of the following form:

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

   The installer performs the following 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.

When the installation finishes, the installer prompts you to run the configuration script, which configures the network and database connections.

6 Select whether to run the configuration script.

a To run the configuration script in an interactive mode, enter **y** and press Enter.

b To run the configuration script later in an interactive or unattended mode, enter **n** and press Enter.

Configure the Network and Database Connections

After you install vCloud Director on the first member of the server group, you must run the configuration script that creates the network and database connections for this cell. The script creates a response file that you must use when configuring additional members of the server group.

All members of the vCloud Director server group share database connection and other configuration details. When you run the configuration script on the first member of the vCloud Director server group, the script creates a response file that preserves database connections information for use in subsequent server installations.

You can run the configuration script in either an interactive mode or an unattended mode. For an interactive configuration, you run the command without options and the script prompts you for the required setup information. For an unattended configuration, you provide the setup information by using the command options.

If you want to use a single IP address with two different ports for the HTTP service and the console proxy service, you must run the configuration script in an unattended mode.

Note The cell management tool includes subcommands that you can use to change the network and database connection details that you initially configured. Changes you make using these subcommands are written to the global configuration file and the response file. For information about using the cell management tool, see the *vCloud Director Administrator's Guide*.

Prerequisites

- For an interactive configuration, review Interactive Configuration Reference.
- For an unattended configuration, review Unattended Configuration Reference.
- For an unattended configuration, 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`.

Procedure

1 Log in to the vCloud Director server as root.

2 Run the `configure` command:

- For an interactive mode, run the command and, on the prompts, provide the required information.

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

- For an unattended mode, run the command with appropriate options and arguments.

```
/opt/vmware/vcloud-director/bin/configure options –unattended
```

The script validates the information, then:

a Initializes the database and connects the server to it.

b Displays a URL at which you can connect to the **VMware vCloud Director Setup** wizard after the vCloud Director service starts.

c Offers to start the vCloud Director cell.

3 (Optional) Take a note of the **VMware vCloud Director Setup** wizard URL and enter **y** to start the vCloud Director service.

You can decide to start the service later by running the `service vmware-vcd start` command.

Database connection information and other reusable information that you supplied during the configuration are preserved in the response 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.

What to do next

Save a copy of the response file at 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 clear texts across a public network.

If you plan to add servers to the server group, mount the shared transfer storage at `/opt/vmware/vcloud-director/data/transfer`.

Interactive Configuration Reference

When you run the `configure` script in an interactive mode, the script prompts you for the following information.

To accept a default value, press Enter.

Table 4-1. Required Information During an Interactive Network and Database Configuration

Required Information	Description
IP address for the HTTP service	Defaults to the first available IP address.
IP address for the console proxy service	Defaults to the first available IP address. **Note** If you want to use a single IP address with two different ports for the HTTP service and the console proxy service, you must run the configuration script in an unattended mode.
Full path to the Java keystore file	For example, `/opt/keystore/certificates.ks`.
Password for the keystore	See Create SSL Certificates.
Private key password for the HTTP SSL certificate	See Create SSL Certificates.
Private key password for the console proxy SSL certificate	See Create SSL Certificates.
Enable remote audit logging to a syslog 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. ■ To skip, press Enter. ■ To enable, enter the syslog host name or IP address.
If you enabled remote audit logging, UDP port of the syslog host	Defaults to 514.
Database type	PostgreSQL or Microsoft SQL Server. Defaults to PostgreSQL.
Host name or IP address of the database server	The server running the database.
Database port	For PostgreSQL, defaults to 5432. For Microsoft SQL Server, defaults to 1433.
Database name	Defaults to vcloud.
If your database type is Microsoft SQL Server, database instance	Defaults to the default instance.
Database user name	See Preparing the vCloud Director Database.

Table 4-1. Required Information During an Interactive Network and Database Configuration (Continued)

Required Information	Description
Database password	See Preparing the vCloud Director Database.
Join or do not participate in the VMware Customer Experience Improvement Program (CEIP)	This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. You can use the cell management tool to join or leave VMware's CEIP for this product at any time. See the "Cell Management Tool Reference" in the *vCloud Director Administrator's Guide*. To join the program, enter **y**. If you prefer not to join the VMware's CEIP program, enter **n**.

Unattended Configuration Reference

When you run the `configure` script in an unattended mode, you provide the setup information at the command line as options and arguments.

Table 4-2. 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 is `/opt/vmware/vcloud-director/etc/global.properties`.
`--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 - 65535	Port number to use for the vCloud Director console proxy service.

Table 4-2. Configuration Utility Options and Arguments (Continued)

Option	Argument	Description
`--database-ssl`	`true` or `false`	If you are using a PostgreSQL database, you can configure the database to require a well-signed SSL connection from vCloud Director. Ignored if `--database-type` is not `postgres`. If you want to configure the PostgreSQL database to use a self-signed or private certificate, see Perform Additional Configurations on the PostgreSQL Database.
`--database-host` (`-dbhost`)	IP address or fully qualified domain name of the vCloud Director database host	See Preparing the vCloud Director Database.
`--database-domain` (`-dbdomain`)	SQL Server database user domain	Optional if `--database-type` is `sqlserver`.
`--database-instance` (`-dbinstance`)	SQL Server database instance	Used if `--database-type` is `sqlserver`.
`--database-name` (`-dbname`)	The database service name	See Preparing the vCloud Director Database.
`--database-password` (`-dbpassword`)	Password for the database user. It can be null.	See Preparing the vCloud Director Database.
`--database-port` (`-dbport`)	Port number used by the database service on the database host	See Preparing the vCloud Director Database.
`--database-type` (`-dbtype`)	The database type. Can be: ■ `postgres` ■ `sqlserver`	See Preparing the vCloud Director Database.
`--database-user` (`-dbuser`)	User name of the database user.	See Preparing the vCloud Director Database.

Table 4-2. Configuration Utility Options and Arguments (Continued)

Option	Argument	Description
`--enable-ceip`	`true` or `false`	This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. You can use the cell management tool to join or leave VMware's CEIP for this product at any time. See the "Cell Management Tool Reference" in the *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 - 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`.
`--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 - 65535	The port on which the `syslog` process monitors the specified server. Defaults to 514 if not specified.

Table 4-2. Configuration Utility Options and Arguments (Continued)

Option	Argument	Description
`--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.
`--unattended-installation` (`-unattended`)	None	Specifies unattended installation
`--keystore-password` (`-w`)	SSL certificate keystore password	SSL certificate keystore password.

Example: Unattended Configuration with Two IP Addresses

The following example command runs an unattended configuration of a vCloud Director server with two different IP addresses for the HTTP service and console proxy service.

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

Example: Unattended Configuration with a Single IP Address

The following example command runs an unattended configuration of a vCloud Director server with a single IP address with two different ports for the HTTP service and console proxy 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 sqlserver -dbhost 10.150.10.78 -dbname mssql-db \
-dbuser vcloud -dbpassword P@55word -k /opt/keystore/certificates.ks -w $3Cret \
-loghost 10.150.10.10 --enable-ceip true -unattended
```

Install vCloud Director on an Additional Member 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.

Important Mixed vCloud Director installations on Linux and vCloud Director appliances in one server group are unsupported.

Prerequisites

- Verify that you can access the response file that was created when you configured the first member of this server group. See Configure the Network and Database Connections.
- Verify that you mounted the shared transfer storage on the first member of the vCloud Director server group at `/opt/vmware/vcloud-director/data/transfer`.

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 media, copy the installation file to a location that is accessible to the target server.
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. Run the installation file.

   To run the installation file, enter the 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.

If you did not install the VMware public key on the target server, the installer prints a warning of the following form:

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

The installer performs the following 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.

When the installation finishes, the installer prompts you to run the configuration script, which configures the network and database connections.

5 Enter **n** and press Enter to reject running the configuration script.

You run the configuration script later by providing the response file as input.

6 Mount the shared transfer storage at `/opt/vmware/vcloud-director/data/transfer`.

All vCloud Director servers in the server group must mount this volume at the same mountpoint.

7 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.

8 Run the configuration script.

- If the console proxy service uses the default port 443, run the command and, on the prompts, provide the IP addresses for the HTTP and the console proxy services.

  ```
  /opt/vmware/vcloud-director/bin/configure -r /responses.properties
  ```

- If the console proxy service uses a custom port, run the command by providing the IP addresses and ports for the HTTP and the console proxy services.

  For example, for a server with a single IP address 10.0.1.61 that uses port 8443 for the console proxy service, run the command:

  ```
  /opt/vmware/vcloud-director/bin/configure -r /responses.properties -cons 10.0.1.61 --console-
  proxy-port-https 8443 -ip 10.0.1.61
  --primary-port-http 80 --primary-port-https 443 -unattended
  ```

The script copies the response file to a location readable by `vcloud.vcloud` and runs the configuration script using the response file as input. The script validates the information, connects the server to the database, and offers to start the vCloud Director cell.

9 If the configuration script does not find valid certificates in the pathname saved in the response file, when prompted, provide the pathname to the certificates and the passwords.

10 (Optional) Enter **y** to start the vCloud Director service.

You can decide to start the service later by running the `service vmware-vcd start` command.

What to do next

Repeat this procedure to add more servers to this server group.

When the vCloud Director services are running on all servers, you must initialize the vCloud Director 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 configuration script finished. See Set Up vCloud Director.
- Use the cell management tool with the `system-setup` subcommand. For information about using the cell management tool, see *vCloud Director Administrator's Guide*.

Set Up vCloud Director

After you install and configure all servers in the vCloud Director server group, you must set up your vCloud Director installation. The vCloud Director setup initializes the vCloud Director database with a license key, system administrator account, and related information.

Before you can start the vCloud Director Web Console, you run the **VMware vCloud Director Setup** wizard, which gathers the information that the Web Console requires to start.

As an alternative to using the **VMware vCloud Director Setup** wizard, to configure the vCloud Director installation, you can use the `system-setup` subcommand of the cell management tool. For information about the cell management tool, see the *vCloud Director Administrator's Guide*.

Prerequisites

- Verify that the vCloud Director services are started on all servers.
- Obtain a vCloud Director product serial number from the VMware License Portal.

Procedure

1 Open a Web browser and go to the URL that the configuration script displayed.

   To discover the URL of the **VMware vCloud Director Setup** wizard, you can also look up the fully qualified domain name associated with the IP address that you specified for the HTTP service during the installation of the first server. To connect to the wizard, go to https://*fully-qualified-domain-name*, for example, https://mycloud.example.com.

   Note Starting the wizard might take a few minutes.

2 Review the Welcome page and click **Next**.

3 Read and accept the licence agreement, and click **Next**.

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

4 Enter your vCloud Director product serial number and click **Next**.

5 Enter a user name, password, and contact information for the vCloud Director system administrator, and click **Next**.

   The vCloud Director system administrator has superuser privileges throughout the cloud. This system administrator can create additional system administrator accounts.

6 Configure the system settings that control how vCloud Director interacts with vSphere and NSX Manager, and click **Next**.

   a In the **System name** text box, enter a name for the vCenter Server folder to use for this vCloud Director installation.

   b In the **Installation ID** text box, set the ID for this vCloud Director installation to use when you create MAC addresses for virtual NICs.

      If you plan to create stretched networks across vCloud Director installations in multisite deployments, consider setting a unique installation ID for each vCloud Director installation.

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

When the configuration process finishes, you are redirected to the vCloud Director Web Console login page.

What to do next

Log in to the vCloud Director Web Console with the system administrator user name and password and begin provisioning your cloud. For information about adding resources to vCloud Director, see the *vCloud Director Administrator's Guide*.

Deploy the vCloud Director Appliance

5

You can create a vCloud Director server group by deploying one or more instances of the vCloud Director appliance. You deploy the vCloud Director appliance as an OVF template by using the vSphere Web Client (Flex).

Important Mixed vCloud Director installations on Linux and vCloud Director appliances in one server group are unsupported.

The vCloud Director appliance is a preconfigured virtual machine that is based on VMware Photon™. The appliance is distributed with a name of the form `VMware vCloud Director-v.v.v.v-nnnnnn_OVF10.ova`, where *v.v.v.v* represents the product version and *nnnnnn* the build number. For example: `VMware vCloud Director-9.5.0.0-9229800_OVA10.ova`.

VMware Photon OS uses the systemd-resolved service that provides network name resolution in the vCloud Director appliance. For information about manually changing the DNS settings of the appliance, see Editing the DNS Settings of the vCloud Director Appliance.

Important Installing any third-party component on the vCloud Director appliance is unsupported. You can install only supported VMware components according to VMware Product Interoperability Matrices. For example, you can install a supported version of a VMware vRealize® Operations Manager™ or VMware vRealize® Log Insight™ monitoring agent.

Prerequisites

- Verify that you have access to the vCloud Director `.ova` file.
- Install and configure the target vCloud Director database. See Preparing the vCloud Director Database.
- Prepare an NFS shared transfer service storage. See Preparing the Transfer Server Storage.
- Install and Configure a RabbitMQ AMQP Broker.

Procedure

1 Start the vCloud Director Appliance Deployment

   To start the appliance deployment, you open the deployment wizard from the vSphere Web Client (Flex).

2 Customize the vCloud Director Appliance and Finish the Deployment

To configure the vCloud Director details, you customize the appliance template.

What to do next

- Configure the public console proxy address, because the vCloud Director appliance uses custom port 8443 for the console proxy service. See Customize Public Endpoints.
- To enter the license key, log in to the vCloud Director Web Console.
- To replace the self-signed certificate that is created during the appliance first boot, you can Create and Import a Signed SSL Certificate.
- To add members to the vCloud Director server group, repeat the procedure.

Start the vCloud Director Appliance Deployment

To start the appliance deployment, you open the deployment wizard from the vSphere Web Client (Flex).

For information about deploying OVF templates in the vSphere Web Client (Flex), see *vSphere Virtual Machine Administration*.

Note Deploying the vCloud Director appliance from the vSphere Client (HTML5) or vCloud Director is unsupported.

Procedure

1 In the vSphere Web Client (Flex), right-click any inventory object and click **Deploy OVF Template**.

2 Enter the path to the vCloud Director `.ova` file and click **Next**.

3 Enter a name for the virtual machine and browse the vCenter Server repository to select a data center or folder on which to deploy the appliance, and click **Next**.

4 Select an ESXi host or cluster on which to deploy the appliance and click **Next**.

5 Review the template details and click **Next**.

6 Read the license agreements, click **Accept**, and click **Next**.

7 Select the disk format and the datastore for the virtual machine configuration files and virtual disks, and click **Next**.

Thick formats improve performance, and thin formats save storage space.

8 From the drop-down menus, select the target network, select the IP allocation settings, and click **Next**.

You are redirected to the **Customize template** page to configure the vCloud Director details.

Customize the vCloud Director Appliance and Finish the Deployment

To configure the vCloud Director details, you customize the appliance template.

When you deploy the vCloud Director appliance as a first member of the server group, you configure the network properties, the appliance settings, the database connections, and the initial system settings. When you deploy the vCloud Director appliance as a subsequent member of a server group, you configure only the network properties and the appliance settings for the new server.

Important Mixed vCloud Director installations on Linux and vCloud Director appliances in one server group are unsupported.

Procedure

1 Expand the **Network Properties** section, enter the IP address for the appliance, and, optionally, set the network details.

2 Expand the **VCD Appliance Settings** section and configure the appliance.

Configuration Property	Description
Enable SSH	Disabled by default.
Initial root password	The root password for the appliance.
NFS mount for transfer file location	See Preparing the Transfer Server Storage.
NTP Server	The host name or IP address of the NTP server to use.

Note For information about changing the date, time, or time zone of the appliance, see https://kb.vmware.com/kb/59674.

3 If you are deploying the first member of a server group, expand the **VCD Configure** section and enter the database details.

Configuration Property	Description
DB host name or IP to connect to	The server running the database.
DB password for the db_user	See Preparing the vCloud Director Database.
DB type to connect to	`postgres` or `mssql`.
DB user to be used to connect with	See Preparing the vCloud Director Database. Defaults to `vcloud`.
Database name to connect to	See Preparing the vCloud Director Database. Defaults to `vcloud`.

Note You cannot configure the database port during the vCloud Director appliance deployment. PostgreSQL databases are configured with the default port 5432, Microsoft SQL databases are configured with the default port 1433. You can set a custom database port after the successful deployment of the appliance by using cell management tool. For information about updating the database connection properties, see the *vCloud Director Administrator's Guide*.

4 If you are deploying the first member of a server group, expand the **VCD First Run Wizard Setup** section, create the **system administrator** account, and configure the system settings.

Configuration Property	Description
Admin Full Name	The full name of the system administrator
Admin User Name	The user name for the system administrator
Admin email	The email address of the system administrator
Admin user password	The password for the system administrator
Installation ID	The ID for this vCloud Director installation to use when you create MAC addresses for virtual NICs. If you plan to create stretched networks across vCloud Director installations in multisite deployments, consider setting a unique installation ID for each vCloud Director installation.
System name	The name for the vCenter Server folder to use for this vCloud Director installation.

5 Click **Next**.

6 On the **Ready to Complete** page, review the configuration settings for the vCloud Director appliance, and click **Finish** to start the deployment.

What to do next

Power on the newly created virtual machine.

Note If vCloud Director fails to start, to determine whether the cell fails to start after the appliance finishes booting, examine the first boot log at `/opt/vmware/var/log/firstboot`.

After you Install vCloud Director or Deploy the vCloud Director Appliance

6

After you create the vCloud Director server group, you can install Microsoft Sysprep files and Cassandra database. If you are using a PostreSQL database, you can configure SSL and adjust some parameters on the database.

This chapter includes the following topics:

- Perform Additional Configurations on the PostgreSQL Database
- Customize Public Endpoints
- Install Microsoft Sysprep Files on the Servers
- Install and Configure a Cassandra Database for Storing Historic Metric Data
- Editing the DNS Settings of the vCloud Director Appliance

Perform Additional Configurations on the PostgreSQL Database

After creating your vCloud Director server group, you can configure the PostgreSQL database to require SSL connections from the vCloud Director cells and adjust some database parameters for optimal performance.

The most secure connections require a well-signed SSL certificate, which includes a complete trust chain rooted in a well-known public certificate authority. Alternatively, you can use a self-signed SSL certificate or an SSL certificate that is signed by a private certificate authority, but you must import that certificate to the vCloud Director truststore.

To obtain optimal performance for your system specification and requirements, you can adjust the database configurations and autovacuum parameters in the database configuration file.

Procedure

1 Configure SSL connections between vCloud Director and the PostgreSQL database.

   a If you used a self-signed or private certificate for the PostgreSQL database, from each vCloud Director cell, run the command to import the database certificate to the vCloud Director truststore.

```
 [root@cell1 /opt/vmware/vcloud-
director/bin]#cell-management-tool import-trusted-certificates --source path_to_self-
signed_or_private_cert
```

   b Run the command to enable SSL connections between vCloud Director and PostgreSQL.

```
 [root@cell1 /opt/vmware/vcloud-director/bin]#
 cell-management-tool reconfigure-database --database-ssl true
```

   You can run the command against all cells in the server group by using the --private-key-path option.

```
 [root@cell1 /opt/vmware/vcloud-director/bin]#
 cell-management-tool reconfigure-database --database-ssl true  --private-key-path
path_to_private_key
```

   For more information about using the cell management tool, see the *vCloud Director Administrator's Guide*.

2 Edit the database configurations in the `postgresql.conf` file for your system specification.

   For example, for a system with 16 GB of memory, you can use the following fragment.

```
max_connections = 500
# Set effective cache size to 50% of total memory.
effective_cache_size = 8GB
# Set shared buffers to 25% of total memory
shared_buffers = 4GB
```

3 Edit the autovacuum parameters in the `postgresql.conf` file for your requirements.

   For typical vCloud Director workloads, you can use the following fragment.

```
autovacuum = on
track_counts = on
autovacuum_max_workers = 3
autovacuum_naptime = 1min
autovacuum_vacuum_cost_limit = 2400
```

   The system sets a custom `autovacuum_vacuum_scale_factor` value for the activity and the `activity_parameters` tables.

What to do next

If you edited the `postgresql.conf` file, you must restart the database.

Customize Public Endpoints

To fulfill load balancer or proxy requirements, you can change the default endpoint Web addresses for the vCloud Director Web Console, vCloud API, Tenant Portal, and console proxy.

If you deployed the vCloud Director appliance, you must configure the vCloud Director public console proxy address, because the appliance uses a single IP address with custom port 8443 for the console proxy service. See Step 5c.

Prerequisites

Only the **system administrator** can customize public endpoints.

Procedure

1. Click the **Administration** tab and, in the left pane, click **Public Addresses**.
2. Select **Customize Public Endpoints**.

   Deselecting this check box reverts all endpoints to their default values, which are not shown on the page.
3. To customize the vCloud REST API and OpenAPI URLs, edit the **API** endpoints.
   a. Enter a custom HTTP base URL.

      For example, if you set the HTTP base URL to **`http://vcloud.example.com`**, you can access the vCloud API at `http://vcloud.example.com/api`, and you can access the vCloud OpenAPI at `http://vcloud.example.com/cloudapi`.

   b. Enter a custom HTTPS REST API base URL and click **Browse** to upload the certificates that establish the trust chain for that endpoint.

      For example, if you set the HTTPS REST API base URL to **`https://vcloud.example.com`**, you can access the vCloud API at `https://vcloud.example.com/api`, and you can access the vCloud OpenAPI at `https://vcloud.example.com/cloudapi`.

      The certificate chain must match the certificate used by the service endpoint, which is either the certificate uploaded to each vCloud Director cell keystore with alias `http` or the load balancer VIP certificate if an SSL termination is used. The certificate chain must include an endpoint certificate, intermediate certificates, and a root certificate in `PEM` format without a private key.

4 To customize the vCloud Director Tenant Portal URLs, edit the **Tenant Portal** endpoints.

- To configure the vCloud Director Tenant Portal to use the same endpoints and certificate chain that you specified in Step 3, select **Copy API URL Settings**.
- To configure the vCloud Director Tenant Portal to use different endpoints and certificate chain, perform the following steps.

  a Deselect **Copy API URL Settings**.

  b Enter a custom HTTP base URL.

  For example, if you set the HTTP base URL to **`http://vcloud.example.com`**, you can access the Tenant Portal at `http://vcloud.example.com/tenant/`*`org_name`*.

  c Enter a custom HTTPS REST API base URL and click **Browse** to upload the certificates that establish the trust chain for that endpoint.

  For example, if you set the HTTPS REST API base URL to **`https://vcloud.example.com`**, you can access the Tenant Portal at `https://vcloud.example.com/tenant/`*`org_name`*.

  The certificate chain must match the certificate used by the service endpoint, which is either the certificate uploaded to each vCloud Director cell keystore with alias `http` or the load balancer VIP certificate if an SSL termination is used. The certificate chain must include an endpoint certificate, intermediate certificates, and a root certificate in `PEM` format without a private key.

5 To customize the vCloud Director Web Console URLs and the console proxy address, edit the **Web Console** endpoints.

   a Enter a custom vCloud Director public URL for HTTP connections.

   The URL must include `/cloud`.

   For example, if you set the vCloud Director public URL to **`http://vcloud.example.com/cloud`**, you can access the vCloud Director Web Console at `http://vcloud.example.com/cloud`.

   b Enter a custom REST API URL for HTTPS connections and click **Browse** to upload the certificates that establish the trust chain for that endpoint.

   The URL must include `/cloud`.

   For example, if you set the base URL to **`https://vcloud.example.com`**, you can access the vCloud Director Web Console at `https://vcloud.example.com/cloud`.

   The certificate chain must match the certificate used by the service endpoint, which is the certificate uploaded to each vCloud Director cell keystore with alias `consoleproxy`. SSL termination of console proxy connections at a load balancer is not supported. The certificate chain must include an endpoint certificate, intermediate certificates, and a root certificate in `PEM` format without a private key.

   c Enter a custom vCloud Director public console proxy address.

   This address is the fully qualified domain name (FQDN) of the vCloud Director server or load-balancer with the port number. The default port is 443.

   Important The vCloud Director appliance uses custom port 8443 for the console proxy service.

   For example, for a vCloud Director appliance with FQDN vcloud.example.com, enter **`vcloud.example.com:8443`**.

   The vCloud Director Web Console uses the console proxy address when opening a remote console window on a VM.

6 To save your changes, click **Apply**.

Install Microsoft Sysprep Files on the Servers

If your cloud requires guest customization support for certain older Microsoft 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 6-1. 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.

Install and Configure a Cassandra Database for Storing Historic Metric Data

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 Cassandra cluster.

Cassandra is an open-source database that you can use to provide the backing store for a scalable, high-performance solution for collecting time series data like virtual machine metrics. If you want vCloud Director to support retrieval of historic metrics from virtual machines, you must install and configure a Cassandra cluster, and use the `cell-management-tool` to connect the cluster to vCloud Director. Retrieval of current metrics does not require optional database software.

Prerequisites

- Verify that vCloud Director is installed and running before you configure the optional database software.
- If you are not already familiar with Cassandra, review the material at http://cassandra.apache.org/.
- See the *vCloud Director Release Notes* for a list of Cassandra releases supported for use as a metrics database. You can download Cassandra from http://cassandra.apache.org/download/.
- Install and configure the Cassandra cluster :
  - The Cassandra cluster must include least four virtual machines deployed on two or more hosts.
  - Two Cassandra seed nodes are required.
  - Enable Cassandra client-to-node encryption. See http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html.
  - Enable Cassandra user authentication. See http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html.
  - Enable Java Native Access (JNA) version 3.2.7 or later on each Cassandra cluster.
  - Cassandra node-to-node encryption is optional.
  - Use of SSL with Cassandra is optional. If you decide not to enable SSL for Cassandra, you must set the configuration parameter `cassandra.use.ssl` to `0` in the `global.properties` file on each cell (`$VCLOUD_HOME/etc/global.properties`)

Procedure

1 Use the `cell-management-tool` utility to configure a connection between vCloud Director and the nodes in the Cassandra cluster.

   In the following example command, *node1-ip*, *node2-ip*, *node3-ip*, and *node4-ip* are the IP address of the members of the Cassandra cluster. The default port (9042) is used. Metrics data is retained for 15 days.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool cassandra --configure --create-schema \
--cluster-nodes node1-ip,node2-ip,node3-ip, node4-ip \
--username admin --password 'P@55w0rd' --ttl 15
```

   For information about using the cell management tool, see the *vCloud Director Administrator's Guide*.

2 (Optional) If you are upgrading vCloud Director from version 9.1, use the `cell-management-tool` to configure the metrics database to store rolled-up metrics.

   Run a command similar to the following example:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool cassandra --add-rollup \
--username admin --password 'P@55w0rd'
```

3 Restart each vCloud Director cell.

Editing the DNS Settings of the vCloud Director Appliance

The vCloud Director appliance is based on Photon OS, which uses the systemd-resolved service to resolve domain names, IP addresses, and network names. The systemd-resolved daemon creates and maintains the `/etc/resolv.conf` file that stores the DNS settings.

After the deployment, you can change the DNS settings of the vCloud Director appliance, for example, you can change the DNS timeout and retry values. To change the DNS settings of the appliance, you must manually manage the `/etc/resolv.conf` file by removing the symlink and replacing it with a regular file containing a valid `resolv.conf` specification. For information about managing the `/etc/resolv.conf` file, see https://www.freedesktop.org/software/systemd/man/systemd-resolved.service.html#/etc/resolv.conf.

Upgrading vCloud Director 7

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

You can use the vCloud Director installer for Linux to upgrade a vCloud Director installation that consists of vCloud Director appliances or vCloud Director installations on a supported Linux OS. You can either Perform an Orchestrated Upgrade of a vCloud Director Installation or Manually Upgrade a vCloud Director Installation. With the orchestrated upgrade, you run a single command which upgrades all cells in the server group and the database. With the manual upgrade, you upgrade each cell and the database in a sequence.

Starting with vCloud Director 9.5:

- Oracle databases are unsupported. If your existing vCloud Director installation uses an Oracle database, see the Workflow for Upgrading a vCloud Director Installation with an Oracle Database.
- Enabling and disabling ESXi hosts is unsupported. Before starting the upgrade, you must enable all ESXi hosts. You can put ESXi hosts in maintenance mode by using the vSphere Web Client.
- vCloud Director uses Java 8 Update 181, which introduces improved LDAP support. If you are using an LDAPS server, to avoid LDAP login failures, you must verify that you have a properly constructed certificate. For information, see the *Java 8 Release Changes* at https://www.java.com.

When you are upgrading vCloud Director, the new version must be compatible with the following components of your existing installation:

- The database software you are currently using for the vCloud Director database.

  If your existing vCloud Director installation uses an Oracle database, see the Workflow for Upgrading a vCloud Director Installation with an Oracle Database.
- The VMware vSphere® release you are currently using.
- The VMware NSX® release that you are currently using.

For information about upgrade paths and compatibility of vCloud Director with other VMware products and with third-party databases, refer to the *VMware Product Interoperability Matrices* at http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. If you plan to upgrade vSphere or NSX components as part of the vCloud Director upgrade, you must upgrade them Chapter 8 After you Upgrade vCloud Director.

After you upgrade at least one vCloud Director server, you can upgrade the 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 verify that no tasks are active on any 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 support are copied to the new installation.

The upgrade requires sufficient vCloud Director downtime to upgrade all servers in the server group and the database. If you are using a load balancer, you can configure it to a return a message, for example, `The system is offline for upgrade.`

Workflow for Upgrading a vCloud Director Installation with an Oracle Database

Before upgrading a vCloud Director installation that uses an Oracle database, you must migrate the database to PostgreSQL from vCloud Director version 9.1.

1 If your current vCloud Director version is earlier than 9.1, upgrade to version 9.1.

   For information about upgrading vCloud Director to version 9.1, see the *vCloud Director Installation and Upgrade Guide* 9.1.

2 When your vCloud Director installation is of version 9.1, migrate the Oracle database to a PostreSQL database.

   For information about migrating to a PostgreSQL database, see the cell management tool reference in the *vCloud Director Administrator's Guide* documentation.

3 Upgrade your vCloud Director installation from version 9.1. You can either Perform an Orchestrated Upgrade of a vCloud Director Installation or Manually Upgrade a vCloud Director Installation.

This chapter includes the following topics:

- Perform an Orchestrated Upgrade of a vCloud Director Installation
- Manually Upgrade a vCloud Director Installation
- Database Upgrade Utility Reference

Perform an Orchestrated Upgrade of a vCloud Director Installation

You can upgrade all cells in the server group and the shared database by running the vCloud Director installer with the `--private-key-path` option. If your vCloud Director cells run in vCloud Director appliances, to upgrade the vCloud Director installation, you must perform an orchestrated upgrade.

You can use the vCloud Director installer for Linux to upgrade a vCloud Director installation that consists of vCloud Director appliances or vCloud Director installations on a supported Linux OS.

vCloud Director for Linux is distributed as a digitally signed 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.

When you run the vCloud Director installer with the `--private-key-path` option, you can add other command options of the `upgrade` utility, for example, `--maintenance-cell`. For information about the database `upgrade` utility options, see Database Upgrade Utility Reference.

Prerequisites

- Verify that your vCloud Director database, the vSphere components, and the NSX components are compatible with the new version of vCloud Director.

  Important If your existing vCloud Director installation uses an Oracle database, verify that you migrated to a PostgreSQL database from vCloud Director version 9.1. See the Workflow for Upgrading a vCloud Director Installation with an Oracle Database.

- Verify that you have superuser credentials for the target server.
- If you want the installer to 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.
- Verify that you have a valid license key to use the version of the vCloud Director software to which you are upgrading.
- Verify that all cells permit SSH connections from the superuser without a password. To perform a verification, you can run the following Linux command:

  ```
  sudo -u vcloud ssh -i private-key-path root@cell-ip
  ```

  This example sets your identity to `vcloud`, then makes an SSH connection to the cell at *cell-ip* as root but does not supply the root password. If the private key in *private-key-path* on the local cell is readable by user `vcloud.vcloud` and the corresponding public key is present in the `authorized-keys` file for the root user at *cell-ip* the command succeeds.

  Note The `vcloud` user, `vcloud` group, and `vcloud.vcloud` account are created by the vCloud Director installer for use as an identity with which vCloud Director processes run. The `vcloud` user has no password.

- Verify that you all ESXi hosts are enabled. Starting with vCloud Director 9.5, disabled ESXi hosts are unsupported.
- Verify that all servers in the server group can access the shared transfer server storage. See Preparing the Transfer Server Storage.

- If your vCloud Director installation uses an LDAPS server, to avoid LDAP login failures after the upgrade, verify that you have a properly constructed certificate for Java 8 Update 181. For information, see the *Java 8 Release Changes* at https://www.java.com.
- Shut down the vCloud Director services on each cell in the server group. You can use the `cell` subcommand of the cell management tool

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

  For more information about managing a cell, see the cell management reference in the *vCloud Director Administrator's Guide*.

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 media, copy the installation file to a location that is accessible to the target server.
3. Verify that the checksum of the download matches the checksum 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 checksum shown on the download page. A Linux command of the following form displays the checksum for *installation-file*.

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

   The command returns the installation file checksum that must match the MD5 checksum 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 with the `--private-key-path` option and the pathname to the private key of the target cell.

   You can add other command options of the database `upgrade` utility.

   ```
   ./installation-file --private-key-path /vcloud/.ssh/id_rsa
   ```

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

   The installer detects an earlier version of vCloud Director and prompts you to confirm the upgrade.

   If the installer detects a version of vCloud Director that is equal to or later than the version in the installation file, it displays an error message and exits.

6 Enter **y** and press Enter to confirm the upgrade.

The installer initiates the following multi-cell upgrade workflow.

1 Verifies that the current cell host meets all requirements.

2 Unpacks the vCloud Director RPM package.

3 Upgrades vCloud Director software on the current cell.

4 Upgrades the vCloud Director database.

5 Upgrades vCloud Director software on each of the remaining cells, then restarts vCloud Director services on the cell.

6 Restarts vCloud Director services on the current cell.

What to do next

Start the vCloud Director services on all cells in the server group.

You can now Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System, then Upgrade vCenter Server Systems, ESXi Hosts, and NSX Edges.

Manually Upgrade a vCloud Director Installation

You can upgrade a single cell by running the vCloud Director installer without command options. Before you restart an upgraded cell, you must upgrade the database schema. You upgrade the database schema after upgrading at least one cell in the server group.

You can use the vCloud Director installer for Linux to upgrade a vCloud Director installation that consists of vCloud Director appliances or vCloud Director installations on a supported Linux OS.

For a multi-cell vCloud Director installation, instead of manually upgrading each cell and the database in a sequence, you can Perform an Orchestrated Upgrade of a vCloud Director Installation.

Prerequisites

- Verify that your vCloud Director database, the vSphere components, and the NSX components are compatible with the new version of vCloud Director.

  Important If your existing vCloud Director installation uses an Oracle database, verify that you migrated to a PostgreSQL database from vCloud Director version 9.1. See the Workflow for Upgrading a vCloud Director Installation with an Oracle Database.

- Verify that you have superuser credentials for the servers in your vCloud Director server group.
- If you want the installer to 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.
- Verify that you have a valid license key to use the version of the vCloud Director software to which you are upgrading.
- Verify that you all ESXi hosts are enabled. Starting with vCloud Director 9.5, disabled ESXi hosts are unsupported.
- Shut down the vCloud Director services on each cell in the server group. You can use the `cell` subcommand of the cell management tool

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

  For more information about managing a cell, see the cell management reference in the *vCloud Director Administrator's Guide*.

Procedure

1. Upgrade a vCloud Director Cell

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

2. Upgrade the vCloud Director Database

   From an upgraded vCloud Director server, you run a tool that upgrades the vCloud Director database. You must not restart any upgraded vCloud Director server before upgrading the shared database.

What to do next

After you upgraded all vCloud Director servers in the server group and the database, you can start the vCloud Director services on all cells.

You can Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System, after which you can Upgrade vCenter Server Systems, ESXi Hosts, and NSX Edges.

Upgrade a vCloud Director Cell

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

vCloud Director for Linux is distributed as a digitally signed 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.

For a multi-cell vCloud Director installation, you must run the vCloud Director installer on each member of the vCloud Director server group.

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 media, copy the installation file to a location that is accessible to the target server.
3. Verify that the checksum of the download matches the checksum 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 checksum shown on the download page. A Linux command of the following form displays the checksum for *installation-file*.

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

   The command returns the installation file checksum that must match the MD5 checksum 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. Run the installation file.

   To run the installation file, enter the 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.

If the installer detects a version of vCloud Director that is equal to or later than the version in the installation file, it displays an error message and exits.

If the installer detects an earlier version of vCloud Director, it prompts you to confirm the upgrade.

6 Enter **y** and press Enter to confirm the upgrade.

The installer initiates the following upgrade workflow.

a Verifies that the host meets all requirements.

b Unpacks the vCloud Director RPM package.

c After all active vCloud Director jobs on the cell finish, stops vCloud Director services on the server and upgrades the installed vCloud Director software.

If you did not install the VMware public key on the target server, the installer displays a warning of the following form:

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

When changing the existing `global.properties` file on the target server, the installer displays a warning of the following form:

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

Note If you previously updated the existing `global.properties` file, you can retrieve the changes from `global.properties.rpmnew`.

7 (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	To preserve your changes, merge `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` with the existing `/opt/vmware/vcloud-director/etc/log4j.properties` file.

When the vCloud Director upgrade finishes, the installer displays a message with information about the location of the old configuration files. Then the installer prompts you to run the database upgrade tool.

What to do next

If not upgraded yet, you can upgrade the vCloud Director database.

Repeat this procedure on each vCloud Director cell in the server group.

Important Do not start the vCloud Director services until you upgrade all cells in the server group and the database.

Upgrade the vCloud Director Database

From an upgraded vCloud Director server, you run a tool that upgrades the vCloud Director database. You must not restart any upgraded vCloud Director server before upgrading the shared database.

Information about all running and recently completed tasks is stored in the vCloud Director database. Because a database upgrade invalidates this task information, the database upgrade utility verifies that no tasks are running when the upgrade process begins.

All cells in a vCloud Director server group share the same database. Regardless of how many cells you are upgrading, you upgrade the database only once. After the database is upgraded, vCloud Director cells that are not upgraded cannot connect to the database You must upgrade all cells so that they connect to the upgraded database.

Prerequisites

- Back up your existing database. Use the procedures that your database software vendor recommends.
- Verify that all vCloud Director cells in the server group are stopped. The upgraded cells are stopped during the upgrade process. If there are vCloud Director servers that are not yet upgraded, you can use the cell management tool to quiesce and shut down their services. For information about how to manage a cell by using the cell management tool, see *vCloud Director Administrator's Guide*.
- If your vCloud Director installation uses an Oracle database, migrate to a PostgeSQL database. For information about migrating to a PostgreSQL database, see the cell management tool reference in *vCloud Director Administrator's Guide*.
- Review the Database Upgrade Utility Reference. The options and arguments are not mandatory.

Procedure

1. Run the database `upgrade` utility with or without options.

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

   If the database upgrade utility detects an incompatible version of NSX Manager, it displays a warning message and cancels the upgrade.
2. On the prompt, enter **y** and press Enter to confirm the database upgrade.
3. On the prompt, enter **y** and press Enter to confirm that you backed up the database.

   If you used the `--backup-completed` option, the utility skips this prompt.

4 If the utility detects an active cell, on the prompt to continue, enter **n** to exit the shell, then verify that no cells are running and retry the upgrade from Step 1.

The database upgrade tool runs and displays progress messages. When the upgrade finishes, you are prompted to start the vCloud Director service on the current server.

What to do next

Enter **y** and press Enter or start the service at a later time by running the `service vmware-vcd start` command.

You can start the services of the upgraded vCloud Director servers.

You can upgrade the rest vCloud Director members of the server group and start their services. See Upgrade a vCloud Director Cell.

Database Upgrade Utility Reference

When you run the `upgrade` utility, you provide the setup information at the command line as options and arguments.

Table 7-1. Database Upgrade Utility Options and Arguments

Option	Argument	Description
`--backup-completed`	None	Specifies that you have completed a backup of the vCloud Director. When you include this option, the upgrade utility does not prompt you to back up the database.
`--ceip-user`	The username for the CEIP service account.	Upgrade will fail if a user with this username already exists in the System organization. Default: `phone-home-system-account`.
`--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*.

Table 7-1. Database Upgrade Utility Options and Arguments (Continued)

Option	Argument	Description
`--installer-path`	Full pathname to the vCloud Director installation file. The installation file and the directory in which it is stored must be readable by the user vcloud.vcloud.	This product participates in VMware's Customer Experience Improvement Program ("CEIP"). Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth in the Trust & Assurance Center at http://www.vmware.com/trustvmware/ceip.html. You can use the cell management tool to join or leave VMware's CEIP for this product at any time. See the "Cell Management Tool Reference" in the *vCloud Director Administrator's Guide*. Requires `--private-key-path` option.
`--maintenance-cell`	IP address	The IP address of a cell for the upgrade utility to run in maintenance mode during the upgrade. This cell enters maintenance mode before the other cells are shut down and stays in maintenance mode while the other cells are upgraded. After the other cells are upgraded and at least one of them has re-started, this cell is shut down and upgraded. Requires `--private-key-path` option.
`--multisite-user`	The username for the Multi-Site system account.	This account is used by the vCloud Director Multi-Site feature. Upgrade will fail if a user with this username already exists in the System organization. Default: `multisite-system-account`.
`--private-key-path`	pathname	The full pathname to the cell's private key. When you use this option, all cells in the server group will be gracefully shut down, upgraded, and re-started after the database has been upgraded. See Perform an Orchestrated Upgrade of a vCloud Director Installation for more information about this upgrade workflow.
`--unattended-upgrade`	None	Specifies unattended upgrade

If you use the `--private-key-path` option, all cells must be configured to permit `ssh` connections from the superuser without a password. You can use a Linux command line like the one shown here to verify this. This example sets your identity to `vcloud`, then makes an `ssh` connection to the cell at *cell-ip* as `root` but does not supply the root password.

```
sudo -u vcloud ssh -i private-key-path root@cell-ip
```

If the private key in *private-key-path* on the local cell is readable by user `vcloud.vcloud` and the corresponding public key has been added to the `authorized-keys` file for the root user at *cell-ip* the command succeeds.

Note The `vcloud` user, `vcloud` group, and `vcloud.vcloud` account are created by the vCloud Director installer for use as an identity with which vCloud Director processes run. The `vcloud` user has no password.

After you Upgrade vCloud Director

8

After you upgraded all vCloud Director servers and the shared database, you can upgrade the NSX Manager instances that provide network services to your cloud. After that, you can upgrade the ESXi hosts and the vCenter Server instances that are registered to your vCloud Director installation.

You can familiarize with the rights and roles model that vCloud Director 9.5 introduces.

This chapter includes the following topics:

- Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System
- Upgrade vCenter Server Systems, ESXi Hosts, and NSX Edges
- Rights and Roles After the Upgrade

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

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

Upgrading NSX Manager interrupts access to NSX administrative functions but does not interrupt network services. You can upgrade NSX Manager before or after you upgrade vCloud Director, whether or not any vCloud Director cells are running.

For information about upgrading NSX, see the NSX for vSphere documentation at https://docs.vmware.com.

Procedure

1. Upgrade the NSX Manager associated with each vCenter Server registered to your vCloud Director installation.
2. After you have upgraded all your NSX Managers, you can upgrade your registered vCenter Server systems and ESXi hosts.

Upgrade vCenter Server Systems, ESXi Hosts, and NSX Edges

After you upgrade vCloud Director and NSX Manager, you must upgrade the vCenter Server systems and ESXi hosts that are registered to vCloud Director. After you upgrade all attached vCenter Server systems and ESXi hosts, 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.

Procedure

1. Disable the vCenter Server instance.
   a. In the vCloud Director Web Console, click the **Manage and Monitor** tab, and, in the left pane, click **vCenters**.
   b. Right-click the target vCenter Server name and click **Disable**.
   c. Click **Yes**.
2. Upgrade the vCenter Server system.

   For information, see *vCenter Server Upgrade*.
3. Verify all vCloud Director public URLs and certificate chains.
   a. In the vCloud Director Web Console, click the **Administration** tab, and, in the left pane, click **Public Addresses**.
   b. Verify all public addresses.
4. Refresh the vCenter Server registration with vCloud Director.
   a. In the vCloud Director Web Console, click the **Manage and Monitor** tab, and, in the left pane, click **vCenters**.
   b. Right-click the target vCenter Server name and click **Refresh**.
   c. Click **Yes**.

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

See the *VMware ESXi Upgrade*.

Important 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.

a 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.

b Upgrade the host.

c Use the vCenter Server system to reconnect the host.

d 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 at https://docs.vmware.com.
- 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 vCloud 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*.

What to do next

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

Rights and Roles After the Upgrade

vCloud Director 9.5 introduces a new access control model, which includes managing rights bundles and global tenant roles.

Starting with vCloud Director 9.5, service providers can use rights bundles and global tenant roles to manage the rights and roles that are available to each organization.

After you upgrade vCloud Director from version 9.1 or earlier, the system contains the System Rights Bundle, which includes all rights that are available in the system, and a Legacy Rights Bundle for each existing organization. Each Legacy Rights Bundle includes the rights that are available in the associated organization at the time of the upgrade and is published only to this organization. The existing role templates are published to all organizations as global tenant roles, and the existing roles that are unlinked from role templates are available as tenant-specific roles to their organizations.

Note To start using the rights bundles model for an organization, you must delete the corresponding Legacy Rights Bundle.

For information about managing rights and roles, see the *vCloud Director Service Provider Admin Portal Guide*.

Uninstall vCloud Director Software

9

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-phonehome vmware-vcloud-director vmware-vcloud-director-rhel
   ```

   If other installed packages depend on the `vmware-vcloud-director` package, the system prompts you to uninstall those packages before you uninstall vCloud Director.