vCloud Director Installation, Configuration, and Upgrade Guide

28 MAR 2019

VMware Cloud Director 9.7

vmware®

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

https://docs.vmware.com/

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

Contents

vCloud Director Installation, Configuration, and Upgrade Guide

The *vCloud Director Installation, Configuration, 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, Configuration, 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, Configuration, 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, Configuration, and Upgrade Guide*.

Revision	Description
11 JUN 2019	■ Added topic Renew the vCloud Director Appliance Certificates. ■ Added chapter Chapter 9 Using the Replication Manager Tool Suite in a High Availability Cluster Configuration.
10 MAY 2019	■ Added chapter #unique_5. ■ Added topic Using the Log Files to Troubleshoot vCloud Director Updates and Patches. ■ Added topic Checking for vCloud Director Updates Fails. ■ Added topic Installing the Latest Update of vCloud Director Fails.
05 APR 2019	■ Added chapter Chapter 12 Migrating to vCloud Director Appliance. ■ Added topic Restoring a vCloud Director Appliance Environment with a High Availability Database Configuration. ■ Updated topic Appliance Deployments and Database High Availability Configuration to improve the graphics and Step 2 in the workflows. ■ Updated topic Examine the Log Files in the vCloud Director Appliance to add information about the file that contains the deployment OVF parameters.
28 MAR 2019	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.

The vCloud Director software for Linux requires an external database, whereas the vCloud Director appliance uses an embedded PostgreSQL database.

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.

When you migrate an existing vCloud Director installation on Linux to the vCloud Director appliance, you update the vCloud Director software and migrate the database to the embedded database in the appliance.

This chapter includes the following topics:

vCloud Director Architecture

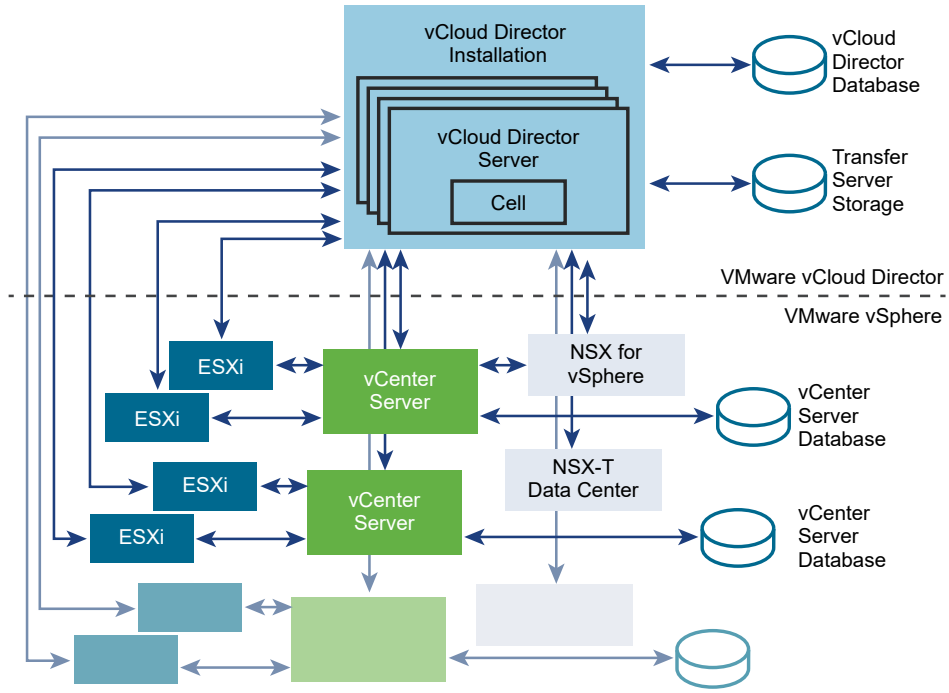
A vCloud Director server group consists of one or more vCloud Director servers installed on Linux or deployments of the vCloud Director appliance. Each server in the group runs a collection of services called a vCloud Director cell. All cells share a single vCloud Director database and a transfer server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

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

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.

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



A vCloud Director server group installed on Linux uses an external database.

A vCloud Director server group that consists of appliance deployments uses the embedded database in the first member of the server group. You can configure a vCloud Director database high availability by deploying two instances of the appliance as standby cells in the same server group. See Appliance Deployments and Database High Availability Configuration.

Figure 1-2. vCloud Director Appliances Comprising an Embedded Database High Availability Cluster

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 the 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 target vCloud Director Linux servers meet at least the minimum requirements for memory and storage detailed in *vCloud Director Release Notes*.
- If you plan to install vCloud Director on Linux, 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 9.7 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 9.7 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

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 its `eth0` 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
```

Reverse DNS lookup of the `eth0` IP address is required for the appliance. The following command must succeed in your environment:

```
host -W 15 -R 1 -T <eth0-IP-address>
```

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
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, deactivate connection to port 443 and activate 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.

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

Port	Protocol	Comments
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

The vCloud Director cells use a database to store shared information. Before you install vCloud Director on Linux, you must install and configure an external vCloud Director database. The vCloud Director appliance uses an embedded PostreSQL database.

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 External PostgreSQL Database.

Configure an External PostgreSQL Database for vCloud Director on Linux

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

Note Only vCloud Director on Linux uses an external database. The vCloud Director appliance uses the embedded PostgreSQL database.

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 External PostgreSQL Database.

Configure an External Microsoft SQL Server Database for vCloud Director for Linux

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

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.

Note Only vCloud Director on Linux uses an external database. The vCloud Director appliance uses the embedded PostgreSQL database.

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. You need specific user and group permissions to configure each cell to mount the NFS-based location and use it as the transfer server storage.

Each member of the server group mounts 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 for which caching of the published content is enabled, 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 have capacity for future expansion.

How vCloud Director Uses the File System Permissions on the Transfer Server Storage Location

For all vCloud Director cells in the vCloud Director server group:

- In standard cloud operations such as uploading items into the catalog, the daemon of the vCloud Director cell writes files to and reads those files from the transfer server storage using the **vcloud** user in the **vcloud** group. The **vcloud** user writes the files with `umask 0077`. When the vCloud Director installer runs and installs the vCloud Director software on a server group member, it also creates the **vcloud** user and **vcloud** group.
- The vCloud Director log data collector script `vmware-vcd-support` can collect the logs from all your vCloud Director cells in one operation and bundle the logs into a single `tar.gz` file. When you run the script, it writes the resulting `tar.gz` file to a directory in the transfer server storage location using the user ID of the user invoking the script. By default, the only user who has permissions to run the script is the **root** user.

- The **root** user on the cell runs the script that writes the `tar.gz` file to the `vmware-vcd-support` directory in the transfer server storage location. If you want to use the multi-cell options to collect the logs from all the cells at once, the **root** user must have a read permission to retrieve the `tar.gz` diagnostic log bundle.

Requirements for Configuring the NFS Server

There are specific requirements for the NFS server configuration, so that vCloud Director can write files to an NFS-based transfer server storage location and read files from it. Because of them, the **vcloud** user can perform the standard cloud operations and the **root** user can perform multi-cell log collection.

- The export list for the NFS server must allow for each server member in your vCloud Director server group to have read-write access to the shared location that is identified in the export list. This capability allows the **vcloud** user to write files to and read files from the shared location.
- The NFS server must allow read-write access to the shared location by the **root** system account on each server in your vCloud Director server group. This capability allows for collecting the logs from all cells at once in a single bundle using the `vmware-vcd-support` script with its multi-cell options. You can meet this requirement by using `no_root_squash` in the NFS export configuration for this shared location.

For example, if the NFS server has the IP address 192.168.120.7 and a directory named vCDspace as the transfer space for the vCloud Director server group with location `/nfs/vCDspace`, to export this directory, you must ensure that its ownership and permissions are **root:root** and **750**. The method for allowing read-write access to the shared location for two cells named vcd-cell1-IP and vcd-cell2-IP is the `no_root_squash` method. You must add a line to the `/etc/exports` file.

```
192.168.120.7/nfs/vCDspace vCD_Cell1_IP_Address(rw,sync,no_subtree_check,no_root_squash)
vCD_Cell2_IP_Address(rw,sync,no_subtree_check)
```

There must be no space between each cell IP address and its immediate following left parenthesis in the export line. If the NFS server reboots while the cells are writing data to the shared location, the use of the `sync` option in the export configuration prevents data corruption in the shared location. The use of the `no_subtree_check` option in the export configuration improves reliability when a subdirectory of a file system is exported.

Each server in the vCloud Director server group must be allowed to mount the NFS share by inspecting the export list for the NFS export. You export the mount by running `exportfs -a` to re-export all NFS shares. NFS daemons `rpcinfo -p localhost` or `service nfs status` must be running on the server.

Considerations When Planning to Upgrade Your vCloud Director Installation to a Later Version

During an upgrade of a vCloud Director server group, you run the installation file for the upgraded version to upgrade all the members of the vCloud Director server group. For convenience, some organizations choose to download the installation file for the upgrade to the transfer server storage location and run it from there, because all the cells have access to that location. Because the **root** user must be used to run the upgrade installation file, if you want to use the transfer server storage location for running an upgrade, you must ensure that the **root** user can run the upgrade installation file when you are performing the upgrade. If you cannot run the upgrade as the **root** user, the file must be copied to another location where it can be run as the **root** user, for example, another directory outside the NFS mount.

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 11 Upgrading vCloud Director and Patching the vCloud Director Appliance.

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 11 Upgrading vCloud Director and Patching the vCloud Director Appliance.

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*.

SSL Certificate Creation and Management for vCloud Director on Linux

4

vCloud Director uses SSL to secure communications between clients and servers. Each vCloud Director server must support two different SSL endpoints, one for HTTPS and one for console proxy communications.

The endpoints can be separate IP addresses or a single IP address with two different ports. Each endpoint requires its own SSL certificate. You can use the same certificate for both endpoints, for example, by using a wildcard certificate.

This chapter includes the following topics:

Before You Create SSL Certificates for vCloud Director on Linux

When 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 You must create the certificates for the server group members only after installing vCloud Director on Linux. The vCloud Director appliance creates self-signed SSL certificates during its first boot.

Procedure

1. Log in to the vCloud Director server as **root**.
2. List the IP addresses for the server.

   Use a command, such as `ifconfig`, to discover this server's IP addresses.

3 For each IP address, run the following command to retrieve the fully qualified domain name (FQDN) to which the IP address is bound.

```
nslookup ip-address
```

4 Make a note of each IP address and the FQDN associated with it. If you are not using a single IP address for both services, decide which IP address is for the HTTPS service and which is for the console proxy service.

You must provide the FQDNs when you create the certificates and the IP addresses when you configure the network and database connections. Make a note of any other FQDNs that can reach the IP address, because you must provide them if you want the certificate to include a Subject Alternative Name.

What to do next

Create the certificates for the two endpoints. You can use certificates signed by a trusted certification authority (CA) or self-signed certificates.

Note CA-signed certificates provide the highest level of trust.

- For information on creating and importing CA-signed SSL certificates, see Create an CA-Signed SSL Certificate Keystore for vCloud Director on Linux.
- For information on creating self-signed SSL certificates, see Create Self-Signed SSL Certificates for vCloud Director on Linux.
- For information on importing your own private key and CA-signed certificate files, see Create CA-Signed SSL Certificate Keystore with Imported Private Keys for vCloud Director on Linux.

Create Self-Signed SSL Certificates for vCloud Director on Linux

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

Each vCloud Director server requires two SSL certificates in a JCEKS keystore file, one for the HTTPS service and one for the console proxy service.

You use the `cell-management-tool` to create the self-signed SSL certificates. The `cell-management-tool` utility is installed on the cell before the configuration agent runs and after you run the installation file. See Install vCloud Director on the First Member of a Server Group.

Important These examples specify a 2048-bit key size, but you should evaluate your installation's security requirements before choosing an appropriate key size. Key sizes less than 1024 bits are no longer supported per NIST Special Publication 800-131A.

Procedure

1 Log in directly or by using an SSH client to the OS of the vCloud Director server as **root**.

2 Run the command to create a public and private key pair for the HTTPS service and for the console proxy service.

```
/opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o
certificates.ks -w passwd
```

The command creates or updates a keystore at `certificates.ks` that has the password `passwd`. The `cell-management-tool` creates the certificates by using the command's default values. Depending on the DNS configuration of your environment, the Issuer CN is set to either the IP address or the FQDN for each service. The certificate uses the default 2048-bit key length and expires one year after creation.

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

Make note of the keystore path name. You need the keystore path name when you run the configuration script to create the network and database connections for the vCloud Director cell. See Configure the Network and Database Connections.

Create an CA-Signed SSL Certificate Keystore for vCloud Director on Linux

Creating and importing CA-signed certificates provides the highest level of trust for SSL communications and helps you secure the connections within your cloud infrastructure.

Each vCloud Director server requires two SSL certificates to secure communications between clients and servers. Each vCloud Director server must support two different SSL endpoints one for HTTPS and one for console proxy communications.

The two endpoints can be separate IP addresses or a single IP address with two different ports. Each endpoint requires its own SSL certificate. You can use the same certificate for both endpoints, for example, by using a wildcard certificate.

Certificates for both endpoints must include an X.500 distinguished name and X.509 Subject Alternative Name extension.

You can use certificates signed by a trusted certificate authority(CA) or self-signed certificates.

You use the `cell-management-tool` to create the self-signed SSL certificates. The `cell-management-tool` utility is installed on the cell before the configuration agent runs and after you run the installation file. See Install vCloud Director on the First Member of a Server Group.

If you already have your own private key and CA-signed certificate files, follow the procedure described in Create CA-Signed SSL Certificate Keystore with Imported Private Keys for vCloud Director on Linux.

Important These examples specify a 2048-bit key size, but you should evaluate your installation's security requirements before choosing an appropriate key size. Key sizes less than 1024 bits are no longer supported per NIST Special Publication 800-131A.

Prerequisites

- Verify that you have access to a computer that has a Java version 8 or later runtime environment, so that you can use the `keytool` command to import the certificates. 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 runtime environment installed. Certificates created with a `keytool` from any other source are not supported for use with vCloud Director. These command-line examples assume that `keytool` is in the user's path.
- Familiarize yourself with the `keytool` command.
- For more details on the available options for the `generate-certs` command, see Generating Self-Signed Certificates for the HTTPS and Console Proxy Endpoints.
- For more details on the available options for the `certificates` command, see Replacing Certificates for the HTTP and Console Proxy Endpoints.

Procedure

1. Log in directly or by using an SSH client to the OS of the vCloud Director server cell as **root**.
2. Run the command to create a public and private key pair for the HTTPS service and for the console proxy service.

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o
   certificates.ks -w keystore_password
   ```

   The command creates or updates a keystore at `certificates.ks` with the specified password. Certificates are created using the command's default values. Depending on the DNS configuration of your environment, the Issuer CN is set to either the IP address or the FQDN for each service. The certificate uses the default 2048-bit key length and expires one year after creation.

   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.

3 Create a certificate signing request for the HTTPS service and for the console proxy service.

Important If you are using separate IP addresses for the HTTPS service and for the console proxy service, adjust the hostnames and IP addresses in the following commands.

a Create a certificate signing request in the `http.csr` file.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass
keystore_password -certreq -alias http -file http.csr -ext
"san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

b Create a certificate signing request in the `consoleproxy.csr` file.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass
keystore_password -certreq -alias consoleproxy -file consoleproxy.csr -ext
"san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

4 Send the certificate signing requests to your Certificate Authority.

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

You obtain the CA-signed certificates.

5 Import the signed certificates into the JCEKS keystore.

a Import the Certificate Authority's root certificate from the `root.cer` file to the `certificates.ks` keystore file.

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore
certificates.ks -alias root -file root_certificate_file
```

b If you received intermediate certificates, import them from the `intermediate.cer` file to the `certificates.ks` keystore file.

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore
certificates.ks -alias intermediate -file intermediate_certificate_file
```

c Import the HTTPS service certificate.

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore
certificates.ks -alias http -file http_certificate_file
```

d Import the console proxy service certificate.

```
keytool -import -storetype JCEKS -storepass keystore_password -keystore
certificates.ks -alias consoleproxy -file console_proxy_certificate_file
```

The commands overwrite the `certificates.ks` file with the newly acquired CA-signed versions of the certificates.

6 To check if the certificates are imported to the JCEKS keystore, run the command to list the contents of the keystore file.

```
keytool -storetype JCEKS -storepass keystore_password -keystore certificates.ks -list
```

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

What to do next

- If you have not yet configured your vCloud Director instance, run the `configure` script to import the certificates keystore to vCloud Director. See Configure the Network and Database Connections.

  Note 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 need the keystore path name when you run the configuration script.

- If you have already installed and configured your vCloud Director instance, use the `certificates` command of the cell management tool to import the certificates keystore. See Replacing Certificates for the HTTP and Console Proxy Endpoints.

Create CA-Signed SSL Certificate Keystore with Imported Private Keys for vCloud Director on Linux

If you have your own private key and CA-signed certificate files, before importing the keystores to your vCloud Director environment, you must create keystore files in which to import the certificates and the private keys for both the HTTPS and the console proxy service .

Prerequisites

- See Before You Create SSL Certificates for vCloud Director on Linux.
- Verify that you have access to a computer that has a Java version 8 or later runtime environment, so that you can use the `keytool` command to import the certificates. 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 runtime environment installed. Certificates created with a `keytool` from any other source are not supported for use with vCloud Director. These command-line examples assume that `keytool` is in the user's path.
- Familiarize yourself with the `keytool` command.
- Download and install OpenSSL.
- For more details on the available options for the `certificates` command, see Replacing Certificates for the HTTP and Console Proxy Endpoints.

Procedure

1 If you have intermediate certificates, run the command to combine the root CA-signed certificate with the intermediate certificates and create a certificate chain.

```
cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
```

2 Use OpenSSL to create intermediate PKCS12 keystore files for both the HTTPS and the console proxy services with the private key, the certificate chain, the respective alias, and specify a password for each keystore file.

a Create the keystore file for the HTTPS service.

```
openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http
-passout pass:keystore_password -out http.pfx -chain
```

b Create the keystore file for the console proxy service.

```
openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt
-name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx –chain
```

3 Use `keytool` to import the PKCS12 keystores into JCEKS keystore.

a Run the command to import the PKCS12 keystore for the HTTPS service.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks
-deststoretype JCEKS -srckeystore http.pfx -srcstoretype PKCS12 -srcstorepass
keystore_password
```

b Run the command to import the PKCS12 keystore for the console proxy service.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks
-deststoretype JCEKS -srckeystore consoleproxy.pfx -srcstoretype PKCS12 -srcstorepass
keystore_password
```

4 To check if the certificates are imported to the JCEKS keystore, run the command to list the contents of the keystore file.

```
keytool -storetype JCEKS -storepass keystore_password -keystore certificates.ks –list
```

5 Repeat this procedure on all vCloud Director cells in your environment.

What to do next

- If you have not yet configured your vCloud Director instance, run the `configure` script to import the certificates keystore to vCloud Director. See Configure the Network and Database Connections.

  Note 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. You need the keystore path name when you run the configuration script.

- If you have already installed and configured your vCloud Director instance, use the `certificates` command of the cell management tool to import the certificates keystore. See Replacing Certificates for the HTTP and Console Proxy Endpoints.

Install vCloud Director on Linux

5

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 11 Upgrading vCloud Director and Patching the vCloud Director Appliance.

Important Mixed vCloud Director installations on Linux and vCloud Director appliance deployments 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 Before You Create SSL Certificates for vCloud Director on Linux.
- 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.

Results

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 5-1. 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 Before You Create SSL Certificates for vCloud Director on Linux.
Private key password for the HTTP SSL certificate	See Before You Create SSL Certificates for vCloud Director on Linux.
Private key password for the console proxy SSL certificate	See Before You Create SSL Certificates for vCloud Director on Linux.
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.

Table 5-1. Required Information During an Interactive Network and Database Configuration (continued)

Required Information	Description
If your database type is Microsoft SQL Server, database instance	Defaults to the default instance.
Database user name	See Preparing the vCloud Director Database.
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 5-2. 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 5-2. 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 External 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 5-2. 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 5-2. 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
```

Protect and Reuse the Response File

Network and database connection details that you configure on the first vCloud Director cell are saved in a response file. This file contains sensitive information that you must reuse when you add servers to the server group. You must preserve the file at a secure location.

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

Important The cell management tool includes subcommands that you can use to make changes in the network and database connection details that you initially specified. Changes you make using these tools are written to the global configuration file and the response file, so you must be sure to have the response file in place (in `/opt/vmware/vcloud-director/etc/responses.properties`) and writable before you use any of the commands that can modify it.

Procedure

1. Protect the response file.

   Save a copy of the 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 text across a public network.

2. Reuse the response file.

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

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

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

   The installer creates this user and group.

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

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

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

What to do next

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

Install vCloud Director 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 appliance deployments 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.

a Run the `configure` command by providing the response file pathname.

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

The script copies the response file to a location readable by `vcloud.vcloud` and runs the configuration script using the response file as input.

b On the prompts, provide the IP addresses for the HTTP and the console proxy services.

c 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.

The script validates the information, connects the server to the database, and offers to start the vCloud Director cell.

9 (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

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**.

Results

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*.

Deploying the vCloud Director Appliance

6

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 by using the vSphere Client (HTML5), the vSphere Web Client (Flex), or VMware OVF Tool.

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

The vCloud Director appliance is a preconfigured virtual machine that is optimized for running the vCloud Director services.

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-9.7.0.0-9229800_OVA10.ova`.

The vCloud Director appliance package contains the following software:

- VMware Photon™ OS
- The vCloud Director group of services
- PostgreSQL 10

The primary-small and standby-small vCloud Director appliance sizes are suitable for lab or test systems. The primary-large and standby-large sizes meet the minimum sizing requirements for production systems. Depending on the workload, you might need to add additional resources.

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.

Appliance Database Configuration

Starting with version 9.7, the vCloud Director appliance includes an embedded PostgreSQL database with a high availability (HA) function. To create an appliance deployment with a database HA cluster, you must deploy one instance of the vCloud Director appliance as a primary cell, and two instances as standby cells. You can deploy additional instances of the vCloud Director appliance in the server group as vCD application cells, which run only the vCloud Director group of services without the embedded database. vCD application cells connect to the database in the primary cell. See Appliance Deployments and Database High Availability Configuration.

By default, the vCloud Director appliance uses TLS, in place of the deprecated SSL, for database connections, including replication. This feature is active immediately after deployment, using a self-signed PostgreSQL certificate. To use a signed certificate from a certificate authority (CA), see Replace a Self-Signed Embedded PostgreSQL and vCloud Director Appliance Management UI Certificate.

Note The vCloud Director appliance does not support external databases.

Appliance Network Configuration

Starting with version 9.7, the vCloud Director appliance is deployed with two networks, `eth0` and `eth1`, so that you can isolate the HTTP traffic from the database traffic. Different services listen on one or both of the corresponding network interfaces.

Service	Port on `eth0`	Port on `eth1`
SSH	22	22
HTTP	80	n/a
HTTPS	443	n/a
PostgreSQL	n/a	5432
Management UI	5480	5480
Console proxy	8443	n/a
JMX	8998, 8999	n/a
JMS/ActiveMQ	61616	n/a

The vCloud Director appliance supports user customization of firewall rules by using `iptables`. To add custom `iptables` rules, you can add your own configuration data to the end of the `/etc/systemd/scripts/iptables` file.

This chapter includes the following topics:

- Appliance Deployments and Database High Availability Configuration
- Prerequisites for Deploying the vCloud Director Appliance
- Deploy the vCloud Director Appliance By Using the vSphere Web Client or the vSphere Client

- Deploying the vCloud Director Appliance by Using VMware OVF Tool

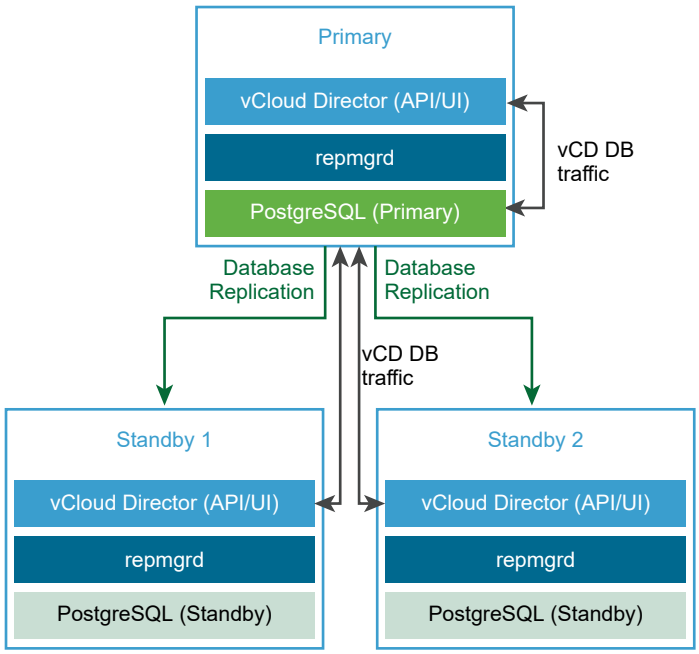
Appliance Deployments and Database High Availability Configuration

The vCloud Director appliance includes an embedded PostgreSQL database. The embedded PostgreSQL database includes the Replication Manager (repmgr) tool suite, which provides a high availability (HA) function to a cluster of PostgreSQL servers. You can create an appliance deployment with a database HA cluster that provides failover capabilities to your vCloud Director database.

You can deploy the vCloud Director appliance as a primary cell, standby cell, or vCD application cell. See Deploy the vCloud Director Appliance By Using the vSphere Web Client or the vSphere Client, Deploying the vCloud Director Appliance by Using VMware OVF Tool, or Deploy the vCloud Director Appliance with Signed Wildcard Certificates for HTTPS and Console Proxy Communication.

To configure HA for your vCloud Director database, when you create your server group, you can configure a database HA cluster by deploying one primary and two standby instances of the vCloud Director appliance.

Figure 6-1. A vCloud Director Appliance Database HA Cluster



Creating a vCloud Director Appliance Deployment with Database HA

To create a vCloud Director server group with a database HA configuration, follow this workflow:

1 Deploy the vCloud Director appliance as a primary cell.

The primary cell is the first member in the vCloud Director server group. The embedded database is configured as the vCloud Director database. The database name is `vcloud`, and the database user is `vcloud`.

2 Verify that the primary cell is up and running.

   a To verify the vCloud Director service health, log in with the **system administrator** credentials to the vCloud Director Web Console at `https://primary_eth0_ip_address/cloud`.

   b To verify the PostgreSQL database health, log in as **root** to the appliance management user interface at `https://primary_eth1_ip_address:5480`.

   The primary node must be in a running status.

3 Deploy two instances of the vCloud Director appliance as standby cells.

   The embedded databases are configured in a replication mode with the primary database.

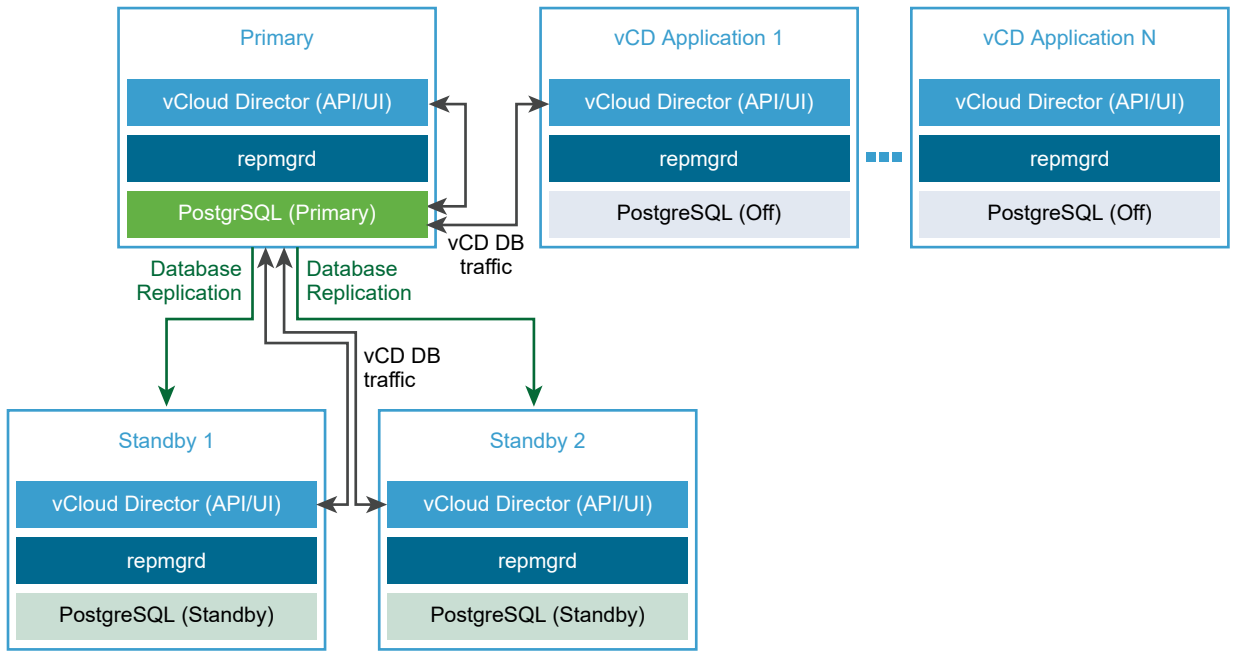
   Note After the initial standby appliance deployment, the replication manager begins synchronizing its database with the primary appliance database. During this time, the vCloud Director database and therefore the vCloud Director UI are unavailable.

4 Verify that all cells in the HA cluster are running.

   See View the Status of the Cells in a Database High Availability Cluster.

5 (Optional) Deploy one or more instances of the vCloud Director appliance as vCD Application cells.

   The embedded databases are not used. The vCD Application cell connects to the primary database.



Creating a vCloud Director Appliance Deployment Without Database HA

Note You can deploy a vCloud Director cluster with one primary cell and no standby cells or application cells. VMware does not provide support for single-cell deployments in a production environment because they are a single source of failure from a database perspective. Single-cell deployments do not receive support for performance or stability related issues.

To create a vCloud Director server without a database HA configuration, follow this workflow:

1 Deploy the vCloud Director appliance as a primary cell.

The primary cell is the first member in the vCloud Director server group. The embedded database is configured as the vCloud Director database. The database name is `vcloud`, and the database user is `vcloud`.

2 Verify that the primary cell is up and running.

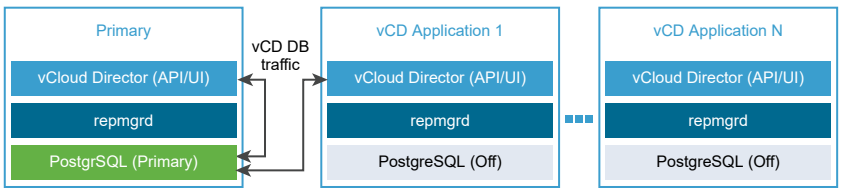
a To verify the vCloud Director service health, log in with the **system administrator** credentials to the vCloud Director Web Console at `https://primary_eth0_ip_address/cloud`.

b To verify the PostgreSQL database health, log in as **root** to the appliance management user interface at `https://primary_eth1_ip_address:5480`.

The primary node must be in a running status.

3 (Optional) Deploy one or more instances of the vCloud Director appliance as vCD Application cells.

The embedded database is not used. The vCD Application cell connects to the primary database.



Prerequisites for Deploying the vCloud Director Appliance

To ensure a successful deployment of the vCloud Director appliance, you must perform some tasks and pre-checks before starting the deployment.

- Verify that you have access to the vCloud Director `.ova` file.

- Before you deploy the primary appliance, prepare an NFS shared transfer service storage. See Preparing the Transfer Server Storage.

  Note The shared transfer service storage must contain neither a `responses.properties` file nor an `appliance-nodes` directory.

- Install and Configure a RabbitMQ AMQP Broker.

vCloud Director Appliance Deployment Methods

- Deploy the vCloud Director Appliance By Using the vSphere Web Client or the vSphere Client
- Deploying the vCloud Director Appliance by Using VMware OVF Tool
- Deploy the vCloud Director Appliance with Signed Wildcard Certificates for HTTPS and Console Proxy Communication

Deploy the vCloud Director Appliance By Using the vSphere Web Client or the vSphere Client

You can deploy the vCloud Director appliance as an OVF template by using the vSphere Web Client (Flex) or the vSphere Client (HTML5).

You must deploy the first member of a vCloud Director server group as a primary cell. You can deploy a subsequent member of a vCloud Director server group as a standby or vCD application cell. See Appliance Deployments and Database High Availability Configuration.

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

For information about deploying OVF templates in vSphere, see *vSphere Virtual Machine Administration*.

As an alternative, you can deploy the appliance by using VMware OVF Tool. See Deploying the vCloud Director Appliance by Using VMware OVF Tool.

Note Deploying the vCloud Director appliance in vCloud Director is unsupported.

Prerequisites

See Prerequisites for Deploying the vCloud Director Appliance.

Procedure

1 vCloud Director Appliance Sizing Guidelines

  Depending on your needs, you can have different configurations of your vCloud Director appliance based server group and different sizes of the vCloud Director virtual appliance instances.

2 Start the vCloud Director Appliance Deployment

To start the appliance deployment, you open the deployment wizard in the vSphere Web Client (Flex) or the vSphere Client (HTML5).

3 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 its `eth0` NIC with custom port 8443 for the console proxy service. See Customize Public Endpoints.
- To add members to the vCloud Director server group, repeat the procedure.
- 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 an CA-Signed SSL Certificate Keystore for vCloud Director on Linux.

vCloud Director Appliance Sizing Guidelines

Depending on your needs, you can have different configurations of your vCloud Director appliance based server group and different sizes of the vCloud Director virtual appliance instances.

Overview

To ensure that the cluster can support an automated failover if a primary cell failure occurs, the minimal vCloud Director deployment must consist of one primary and two standby cells. The environment remains available under any failure scenario where one of the cells goes offline for any reason. If a standby failure occurs, until you redeploy the failed cell, the cluster operates in a fully functional state with some performance degradation. See Appliance Deployments and Database High Availability Configuration.

The vCloud Director appliance has four sizes that you can select during the deployment: Small, Medium, Large, and Extra Large (VVD). The Small appliance size is suitable for lab evaluation and this document does not provide guidance on the Small appliance configuration. The sizing options table provides the specifications for the remaining options and the most suitable use cases for a production environment. The Extra Large configuration matches the VMware Validated Designs (VVD) for Cloud Providers scale profile.

To create larger custom sizes, **system administrators** can adjust the size of the deployed cells.

The smallest recommended configuration for production deployments is a three-node deployment of Medium size virtual appliances.

Note You can deploy a vCloud Director cluster with one primary cell and no standby cells or application cells. VMware does not provide support for single-cell deployments in a production environment because they are a single source of failure from a database perspective. Single-cell deployments do not receive support for performance or stability related issues.

vCloud Director Appliance Sizing Options

You can use the following decision guide to estimate the appliance size for your environment.

	Medium	Large	Extra Large (VVD)
Recommended use cases	Lab or small production environments	Production environment	Production with API integrations and monitoring
vRealize Operations Management Pack deployment in the vCloud Director environment	No	No	Yes
Cassandra VM metrics enablement in vCloud Director	No	No	Yes
Approximate number of concurrent users or clients accessing the API over a peak 30 minute period.	< 50	< 100	< 100
Managed VMs	5000	5000	15000

Configuration Definitions

Note vCloud Director 9.7 and later `primary-large` and `standby-large` appliances, by default, do not have the 16 vCPUs required for a Large HA cluster configuration. If you want to have a Large vCloud Director appliance configuration, after deployment, you must manually change the primary and standby cell vCPUs to 16.

	Medium	Large	Extra Large (VVD)
HA cluster configuration	1 primary + 2 standby cells	1 primary + 2 standby + 1 application cells	1 primary + 2 standby + 2 application cells
vCPUs primary or standby cell	8	16	24
vCPUs application cell	N/A	8	8
RAM primary or standby cell	16 GB	24 GB	32 GB
RAM application cell	N/A	8	8
vCPU to physical core ratio	1:1	1:1	1:1
PostgreSQL customization on primary and standby cells	shared_buffers = '3GB'; effective_cache_size = '9GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '8';	shared_buffers = '5GB'; effective_cache_size = '15GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '16';	shared_buffers = '7GB'; effective_cache_size = '21GB'; work_mem = '8MB'; maintenance_work_mem = '1GB'; max_worker_processes= '24';

How to detect if your system is undersized

In a vCloud Director cell, the CPU or memory use grows and reaches a plateau at a high level, that is, a level near capacity. The vCloud Director cell might also lose the connection to the database.

How to detect if your system number of cells are insufficient

In the `vcloud-container-debug.log` and `cell-runtime.log` files of any of the vCloud Director cells, you see entries similar to `org.apache.tomcat.jdbc.pool.PoolExhaustedException: [pool-jetty-XXXXX] Timeout: Pool empty. Unable to fetch a connection in 20 seconds, none available`. The vCloud Director cell might also lose the connection to the database.

Note Based on the default database connection configuration, all configurations are limited to a maximum of 6 cells of primary, standby and application type.

How to customize the appliance sizing

To customize the sizing of the vCloud Director appliance to one of the supported configurations, after running the vCloud Director appliance deployer, you must follow this procedure on all cells.

1 Verify that you have the necessary number of cells for the selected configuration.

2 Adjust the memory and vCPU of all cells to match one of the supported configuration you want.

   Important The amount of RAM and vCPU must be the same for all primary and standby cells.

3 Log in directly or by using an SSH client to the OS of the primary appliance as **root**.

4 Change the user to **postgres**.

```
sudo -i -u postgres
```

5 Update the `postgresql.auto.conf` configuration file by running the following commands.

Configuration Type	Description

Medium	`psql -c "ALTER SYSTEM set shared_buffers = '3GB';"`
	`psql -c "ALTER SYSTEM set effective_cache_size = '9GB';"`
	`psql -c "ALTER SYSTEM set work_mem = '8MB';"`
	`psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"`
	`psql -c "ALTER SYSTEM set max_worker_processes= '8';"`

Large	`psql -c "ALTER SYSTEM set shared_buffers = '5GB';"`
	`psql -c "ALTER SYSTEM set effective_cache_size = '15GB';"`
	`psql -c "ALTER SYSTEM set work_mem = '8MB';"`
	`psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"`
	`psql -c "ALTER SYSTEM set max_worker_processes= '16';"`

Extra Large	`psql -c "ALTER SYSTEM set shared_buffers = '7GB';"`
	`psql -c "ALTER SYSTEM set effective_cache_size = '21GB';"`
	`psql -c "ALTER SYSTEM set work_mem = '8MB';"`
	`psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"`
	`psql -c "ALTER SYSTEM set max_worker_processes= '24';"`

6 Return to the **root** user by running the `exit` command.

7 Restart the vpostgres process.

```
systemctl restart vpostgres
```

8 Change the user to **postgres** again.

```
sudo -i -u postgres
```

9 For each standby node copy the `postgresql.auto.conf` file to the node and restart the vpostgres process.

a Copy `postgresql.auto.conf` from the primary node to the standby node.

```
scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
```

b Restart the vpostgres process.

```
systemctl restart vpostgres
```

To customize the sizing of the vCloud Director appliance to a custom configuration, after running the vCloud Director appliance deployer, you must follow this procedure on all cells.

1 Log in directly or by using an SSH client to the OS of the primary appliance as **root**.

2 To view and take note of the vCPU information, run the following command.

```
grep -c processor /proc/cpuinfo
```

3 To view and take note of the RAM information, run the following command.

The RAM reported below is in KB and you must convert it to GB by dividing by 1024000.

```
cat /proc/meminfo | grep MemTotal | cut -dk -f1 | awk '{print int($2/1024000)}'
```

4 Calculate the `shared_buffers` value to be one-fourth of the total RAM minus 4GB.

`shared_buffers` = 0.25 * (*total RAM* - 4GB)

5 Calculate the `effective_cache_size` value to be three-fourths of the total RAM minus 4GB.

`effective_cache_size` = 0.75 * (*total RAM* - 4GB)

6 Calculate the `max_worker_processes` value to be number of vCPUs.

7 Change the user to **postgres**.

```
sudo -i -u postgres
```

8 Update the `postgresql.auto.conf` configuration file by running the following commands and substituting the calculated values.

```
psql -c "ALTER SYSTEM set shared_buffers = 'shared_buffers value';"
psql -c "ALTER SYSTEM set effective_cache_size =  'effective_cache_size value';"
psql -c "ALTER SYSTEM set work_mem = '8MB';"
psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';"
psql -c "ALTER SYSTEM set max_worker_processes= 'max_worker_processes value';"
```

9 Return to the **root** user by running the `exit` command.

10 Restart the vpostgres process.

```
systemctl restart vpostgres
```

11 Change the user to **postgres** again.

```
sudo -i -u postgres
```

12 For each standby node copy the `postgresql.auto.conf` file to the node and restart the vpostgres process.

   a Copy `postgresql.auto.conf` from the primary node to the standby node.

   ```
   scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@standby-node-address:/var/vmware/vpostgres/current/pgdata/
   ```

   b Restart the vpostgres process.

   ```
   systemctl restart vpostgres
   ```

Start the vCloud Director Appliance Deployment

To start the appliance deployment, you open the deployment wizard in the vSphere Web Client (Flex) or the vSphere Client (HTML5).

Procedure

1 In the vSphere Web Client or the vSphere Client, 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 and accept the license agreements, and click **Next**.

7 Select the deployment type and size, and click **Next**.

   The primary-small and standby-small vCloud Director appliance sizes are suitable for lab or test systems. The primary-large and standby-large sizes meet the minimum sizing requirements for production systems. Depending on the workload, you might need to add additional resources.

Option	Description
Primary-small	Deploys the appliance with 12 GB of RAM and 2 vCPUs as the first member in a vCloud Director server group. The embedded database in the primary cell is configured as the vCloud Director database. The database name is `vcloud`, and the database user is `vcloud`.
Primary-large	Deploys the appliance with 24 GB of RAM and 4 vCPUs as the first member in a vCloud Director server group. The embedded database in the primary cell is configured as the vCloud Director database. The database name is `vcloud`, and the database user is `vcloud`.

Option	Description
Standby-small	Used to join a primary-small cell in a database HA cluster. Deploys the appliance with 12 GB of RAM and 2 vCPUs as the second or the third member in a vCloud Director server group with a database high availability configuration. The embedded database in a standby cell is configured in a replication mode with the primary database.
Standby-large	Used to join a primary-large cell in a database HA cluster. Deploys the appliance with 24 GB of RAM and 4 vCPUs as the second or the third member in a vCloud Director server group with a database high availability configuration. The embedded database in a standby appliance is configured in a replication mode with the primary database.
vCD Cell Application	Deploys the appliance with 8 GB of RAM and 2 vCPUs as a subsequent member in a vCloud Director server group. The embedded database in a vCD application cell is not used. The vCD application cell connects to the primary database.

Important The primary and the standby cells in a vCloud Director server group must be of the same size. A database HA cluster can consist of one primary-small and two standby-small cells, or consist of one primary-large and two standby-large cells.

After the deployment, you can reconfigure the size of the appliance.

8 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.

9 From the drop-down menus in the **Destination Network** cells, select the target networks for the `eth1` and `eth0` NICs of the appliance.

The source network list might be in reverse order. Verify that you are selecting the correct destination network for each source network.

Important The two destination networks must be different.

10 From the **IP allocation Settigs** drop-down menus, select a **Static-Manual** IP allocation and an **IPv4** protocol.

11 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 customize the vCloud Director appliance, you configure the appliance settings, the database, and the network properties. You configure the initial system settings only when deploying a primary appliance, which is the first member of a server group.

Note Only Step 3 of this procedure is optional. You must complete all other steps to customize the vCloud Director appliance.

Procedure

1 In section **VCD Appliance Settings**, configure the appliance details.

Setting	Description
NTP Server	The host name or IP address of the NTP server to use.
Initial root password	The initial root password for the appliance. Must contain at least eight characters, one uppercase character, one lowercase character, one numeric digit, and one special character. **Important** The initial root password becomes the keystore password. The cluster deployment requires all the cells to have the same root password during the initial deployment. After the boot process finishes, you can change the root password on any desired cell. **Note** The OVF deployment wizard does not validate the initial root password against password criteria.
Expire Root Password Upon First Login	If you want to continue using the initial password after the first login, you must verify that the initial password meets root password criteria. To continue using the initial root password after the first login, deselect this option.
Enable SSH	Deactivated by default.
NFS mount for transfer file location	See Preparing the Transfer Server Storage.

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

2 If you are deploying the first member of a server group, in section **VCD Configure - Required only for "primary" applainces**, enter the database details, create the **system administrator** account, and configure the system settings.

The database name is `vcloud`, and the database user is `vcloud`.

Setting	Description
'vcloud' DB password for the 'vcloud' user	The password for the `vcloud` database user.
Admin User Name	The user name for the **system administrator** account. Defaults to `administrator`.
Admin Full Name	The full name of the **system administrator**. Defaults to `vCD Admin`.
Admin user password	The password for the **system administrator** account.
Admin email	The email address of the **system administrator**.

Setting	Description
System name	The name for the vCenter Server folder to create for this vCloud Director installation. Defaults to `vcd1`.
Installation ID	The ID for this vCloud Director installation to use when you create MAC addresses for virtual NICs. Defaults to `1`. 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.

3 (Optional) In section **Additional Networking Properties**, if your network topology requires it, enter the static routes for the `eth0` and `eth1` network interfaces, and click **Next**.

You might need to provide static routes if you want to reach hosts over a non-default gateway route. For example, management infrastructure is accessible only via `eth1` interface, while the default gateway is on `eth0`. In most cases, this setting can remain empty.

The static routes must be in a comma-separated list of route specifications. A route specification must consist of the IP address of the target gateway and, optionally, a Classless Inter-Domain Routing (CIDR) network specification. For example, **`172.16.100.253 172.16.100.0/19, 172.16.100.253 192.168.100.0/24`**.

4 In section **Networking Properties**, enter the network details for the `eth0` and `eth1` NICs, and click **Next**.

Note All settings are required.

Setting	Description
Default Gateway	The IP address of the default gateway for the appliance.
Domain Name	The domain name, for example, *mydomain.com*.
Domain Search Path	A comma- or space-separated list of domain names for the domain search path of the appliance.
Domain Name Servers	The IP address of the domain name server for the appliance.
eth0 Network IP Address	The IP address for the `eth0` interface.
eth0 Network Mask	The netmask or prefix for the `eth0` interface.
eth1 Network IP Address	The IP address for the `eth1` interface.
eth1 Network Mask	The netmask or prefix for the `eth1` interface.

5 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.

Deploying the vCloud Director Appliance by Using VMware OVF Tool

You can deploy the vCloud Director appliance as an OVF template by using the VMware OVF Tool.

You must deploy the first member of a vCloud Director server group as a primary cell. You can deploy a subsequent member of a vCloud Director server group as a standby or vCD application cell. See Appliance Deployments and Database High Availability Configuration.

For information about installing OVF Tool, see the *VMware OVF Tool Release Notes* document.

For information about using OVF Tool, see the *OVF Tool User's Guide*.

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

When adding additional or replacement appliances to a database cluster, the vCPU and RAM must match those of the existing primary and standby cells in the cluster.

The OVA version of the newly deployed standby must be the same as the existing appliances in the cluster. To view the version of the running appliances, see the About information in the appliance management UI. The appliance is distributed with a name of the form `VMware Cloud 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 Cloud Director-10.2.0.0-9229800_OVA10.ova`.

For information about deploying OVF templates in vSphere, see *vSphere Virtual Machine Administration*.

As an alternative, you can deploy the appliance using the vSphere Client. See Deploy the vCloud Director Appliance By Using the vSphere Web Client or the vSphere Client.

Note Deploying the vCloud Director appliance in vCloud Director is unsupported.

Before running the deployment command, see Prerequisites for Deploying the vCloud Director Appliance.

After you deploy the appliance, view the firstboot log file for warning error messages. See Examine the Log Files in the vCloud Director Appliance.

`ovftool` Command Options and Properties for Deploying the vCloud Director Appliance

Option	Value	Description
`--noSSLVerify`	n/a	Skips SSL verification for vSphere connections.
`--acceptAllEulas`	n/a	Accepts all end-user licenses agreements (EULAs).
`--datastore`	*target_vc_datastore*	The target datastore name on which to store the virtual machine configuration files and virtual disks.
`--allowAllExtraConfig`	n/a	Converts all extra config options to the `VMX` format.
`--net:"eth0 Network"`	*portgroup_on_vc_for_eth0*	The destination network for the appliance `eth0` network. **Important** Must be different from the `eth1` destination network.
`--net:"eth1 Network"`	*portgroup_on_vc_for_eth1*	The destination network for the appliance `eth1` network. **Important** Must be different from the `eth0` destination network.
`--name`	*vm_name_on_vc*	The virtual machine name for the appliance.
`--diskMode`	`thin` or `thick`	The disk format for the virtual machine configuration files and virtual disks.
`--prop:"vami.ip0.VMware_vCloud_Director"`	*eth0_ip_address*	IP address of `eth0`. Used for the UI and API access. On this address, the DNS reverse lookup determines and sets the hostname of the appliance.
`--prop:"vami.ip1.VMware_vCloud_Director"`	*eth1_ip_address*	IP address of `eth1`. Used for accessing internal services including the embedded PostreSQL database service.
`--prop:"vami.DNS.VMware_vCloud_Director"`	*dns_ip_address*	The IP address of the domain name server for the appliance.
`--prop:"vami.domain.VMware_vCloud_Director"`	*domain_name*	The DNS search domain. Appears as the first element in the search path.
`--prop:"vami.gateway.VMware_vCloud_Director"`	*gateway_ip_address*	The IP address of the default gateway for the appliance.
`--prop:"vami.netmask0.VMware_vCloud_Director"`	*netmask*	The netmask or prefix for the `eth0` interface.
`--prop:"vami.netmask1.VMware_vCloud_Director"`	*netmask*	The netmask or prefix for the `eth1` interface.
`--prop:"vami.searchpath.VMware_vCloud_Director"`	*domain_names*	The domain search path of the appliance. A comma or space-separated list of domain names.

Option	Value	Description
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"	true | false	Activates or deactivates the SSH **root** access to the appliance.
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"	true | false	Determines whether to continue or not using the initial password after the first login.
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"	*nfs_ip_address*:*nfs_mount_path*	The IP address and export path of the external NFS server. Used only for a primary cell.
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"	*ip_address*	The IP address of the time server.
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"	*new_root_password*	The initial root password for the appliance. Must contain at least eight characters, one uppercase character, one lowercase character, one numeric digit, and one special character. **Important** The initial root password becomes the keystore password. The cluster deployment requires all the cells to have the same root password during the initial deployment. After the boot process finishes, you can change the root password on any desired cell.
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"	*db_password*	The database password of the **vcloud** user. Used only for a primary cell.
--prop:"vcloudwiz.admin_email.VMware_vCloud_Director"	*email_address*	The email address of the **system administrator** account. Used only for a primary cell.
--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director"	*first_name*	The name for the **system administrator** account. Used only for a primary cell.
--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director"	*admin_password*	The password for the **system administrator** account. Used only for a primary cell.
--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director"	*system_admin_username*	The user name for the **system administrator** account. Used only for a primary cell.
--prop:"vcloudwiz.inst_id.VMware_vCloud_Director"	*ID*	The vCloud Director installation ID. Used only for a primary cell.
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"	*system_name*	The name for the vCenter Server folder to create for this vCloud Director installation.

Option	Value	Description
`--prop:"vcloudnet.routes0.VMware_vCloud_Addresses1"`	*ip_address1 cidr, ip_address2, ...*	Optional. Static routes for the `eth0` interface. Must be a comma-separated list of route specifications. A route specification must consist of a gateway IP address and, optionally, Classless Inter-Domain Routing (CIDR) network specification (prefix/bits). For example, **`172.16.100.253 172.16.100/19, 172.16.200.253`**.
`--prop:"vcloudnet.routes1.VMware_vCloud_Addresses1"`	*ip_address1 cidr, ip_address2, ...*	Optional. Static routes for the `eth1` interface. Must be a comma-separated list of route specifications. A route specification must consist of a gateway IP address and, optionally, Classless Inter-Domain Routing (CIDR) network specification (prefix/bits). For example,**`172.16.100.253 172.16.100/19, 172.16.200.253`**.

Option	Value	Description
`--deploymentOption`	`primary-small`,`primary-large`, `standby-small`, `standby-large`, or `cell`	The appliance type and size that you want to deploy. The primary-small and standby-small appliance sizes are suitable for lab or test systems. The primary-large and standby-large sizes meet the minimum sizing requirements for production systems. Depending on the workload, you might need to add additional resources. ■ `primary-small` deploys the appliance with 12 GB of RAM and 2 vCPUs as the first member in a vCloud Director server group. The embedded database in the primary cell is configured as the vCloud Director database. The database name is `vcloud`, and the database user is `vcloud`. ■ `primary-large` deploys the appliance with 24 GB of RAM and 4 vCPUs as the first member in a vCloud Director server group. The embedded database in the primary cell is configured as the vCloud Director database. The database name is `vcloud`, and the database user is `vcloud`. ■ `standby-small` deploys the appliance with 12 GB of RAM and 2 vCPUs as the second or the third member in a vCloud Director server group with a database high availability configuration. The embedded database in a standby cell is configured in a replication mode with the primary database. ■ `standby-large` deploys the appliance with 24 GB of RAM and 4 vCPUs as the second or the third member in a vCloud Director server group with a database high availability configuration. The embedded database in a standby cell is configured in a replication mode with the primary database. ■ `cell` deploys the appliance with 8 GB of RAM and 2 vCPUs as a subsequent member in a vCloud Director server group. The

Option	Value	Description
		embedded database in a vCD application cell is not used. The vCD application cell connects to the primary database. **Important** The primary and the standby cells in a vCloud Director server group must be of the same size. A database HA cluster can consist of one primary-small and two standby-small cells, or consist of one primary-large and two standby-large cells. After the deployment, you can reconfigure the size of the appliance.
`--powerOn`	*path_to_ova*	Powers on the virtual machine after the deployment.

An Example Command for Deploying the Primary vCloud Director Appliance

Important Before running the VMware OVF Tool command, replace the `vcloudapp.varoot-passwordVMware_vCloud_Director`, `vcloudconf.db_pwdVMware_vCloud_Director`, and `vcloudconf.admin_pwd.VMware_vCloud_Director` passwords with your own secure passwords.

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig  \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
```

```
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_dataceter_name/host/vc_cluster_name
```

An Example Command for Deploying a Standby vCloud Director Appliance

Important Before running the VMware OVF Tool command, replace the `vcloudapp.varoot-password.VMware_vCloud_Director` password with your own secure password.

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig  \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \
--deploymentOption="standby-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_dataceter_name/host/vc_cluster_name
```

vCloud Director Appliance SSL Certificates Creation and Management

7

The vCloud Director appliance uses SSL to secure communications between clients and servers. Each vCloud Director appliance must support two different SSL endpoints - for HTTPS and for console proxy communications.

These endpoints can be separate IP addresses, or a single IP address with two different ports. Each endpoint requires its own SSL certificate. You can use the same certificate (for example a wildcard certificate) for both endpoints.

This chapter includes the following topics:

Deploy the vCloud Director Appliance with Signed Wildcard Certificates for HTTPS and Console Proxy Communication

You can deploy the vCloud Director appliance with signed wildcard certificates. You can use these certificates to secure an unlimited number of servers that are subdomains of the domain name listed in the certificate.

By default, when deploying vCloud Director appliances, vCloud Director generates self-signed certificates and uses them to configure the vCloud Director cell for the HTTPS and console proxy communication.

When you successfully deploy a primary appliance, the appliance configuration logic copies the `responses.properties` file from the primary appliance to the common NFS shared transfer service storage at `/opt/vmware/vcloud-director/data/transfer`. Other appliances deployed for this vCloud Director server group use this file to configure themselves automatically. The `responses.properties` file includes a path to the SSL certificate keystore, which includes the auto-generated self-signed certificates `user.keystore.path`. By default, this path is to a keystore file that is local to each appliance.

After you deploy the primary appliance, you can reconfigure it to use signed certificates. For more information on creating the keystore with signed certificates, see Create and Import CA-Signed SSL Certificates to the vCloud Director Appliance.

If the signed certificates you use on the primary vCloud Director appliance are wildcard signed certificates, these certificates can apply to all other appliances in the vCloud Director server group, that is, standby cells and vCloud Director application cells. You can use the deployment of the appliance with signed wildcard certificates for HTTPS and console proxy communication to configure the additional cells with the signed wildcard SSL certificates.

Prerequisites

- Verify that the keystore containing the signed wildcard SSL certificates for both HTTPS and console proxy aliases is available on the primary appliance, that is, `/opt/vmware/vcloud-director/certificates.ks`.
  - If you need to create keypairs and import CA-signed certificate files, see Create and Import CA-Signed SSL Certificates to the vCloud Director Appliance.
  - If you already have your own private key and CA-signed certificate files, see Import Private Keys and CA-Signed SSL Certificates to the vCloud Director Appliance.
- Verify that the private password for the keys within the keystore matches the password of the keystore. The keystore password must match the initial root password used when deploying all appliances, for example,

```
/opt/vmware/vcloud-director/jre/bin/keytool -keypasswd -alias http_or_consoleproxy
-keystore /opt/vmware/vcloud-director/certificates.ks -storetype jceks -storepass root-
password
```

.

Procedure

1. Copy the new `certificates.ks` file containing the well-signed certs from the primary appliance to the transfer share at `/opt/vmware/vcloud-director/data/transfer/`.
2. Change the owner and the group permissions on the keystore file to **vcloud**.

```
chown vcloud.vcloud /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

3 Verify that the owner of the keystore file has read and write permissions.

```
chmod 0750 /opt/vmware/vcloud-director/data/transfer/certificates.ks
```

4 On the primary appliance, run the command to import the new signed certificates into the vCloud Director instance.

This command also updates the `responses.properties` file in the transfer share, modifying the *user.keystore.path* variable to point to the keystore file in the transfer share.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
vmware/vcloud-director/data/transfer/certificates.ks --keystore-password root-password
```

5 For the new signed certificates to take effect, restart the *vmware-vcd* service on the primary appliance.

```
service vmware-vcd restart
```

6 Deploy the standby cell and application cell appliances, using the initial root password that matches the keystore password.

Results

All newly deployed appliances that use the same NFS shared transfer service storage are configured with the same signed wildcard SSL certificates used by the primary appliance.

Create and Import CA-Signed SSL Certificates to the vCloud Director Appliance

Creating and importing certificates signed by a certificate authority (CA) provides the highest level of trust for SSL communications and helps you secure the connections within your cloud.

Each vCloud Director server requires two SSL certificates to secure communications between clients and servers. Each vCloud Director server must support two different SSL endpoints - for HTTPS and for console proxy communications.

In the vCloud Director appliance, these two endpoints share the same IP address or hostname, but use two distinct ports - `443` for HTTPS and `8443` for console proxy communications. Each endpoint must have its own SSL certificate. You can use the same certificate for both endpoints, for example, by using a wildcard certificate.

Certificates for both endpoints must include an X.500 distinguished name and X.509 Subject Alternative Name extension.

If you already have your own private key and CA-signed certificate files, follow the procedure described in Import Private Keys and CA-Signed SSL Certificates to the vCloud Director Appliance.

Important Upon deployment, the vCloud Director appliance generates self-signed certificates with a 2048-bit key size. You must evaluate your installation's security requirements before choosing an appropriate key size. Key sizes less than 1024 bits are no longer supported per NIST Special Publication 800-131A.

The keystore password used in this procedure is the **root** user password, and it is represented as *root_passwd*.

Prerequisites

Familiarize yourself with the `keytool` command. You use `keytool` to import CA-signed SSL certificates to the vCloud Director appliance. vCloud Director places a copy of `keytool` at `/opt/vmware/vcloud-director/jre/bin/keytool`.

Procedure

1. Log in directly or SSH to the vCloud Director appliance console as **root**.
2. Depending on your environment needs, choose one of the following options.

   When you deploy the vCloud Director appliance, vCloud Director automatically generates self-signed certificates with a 2048-bit key size for the HTTPS service and the console proxy service.

   - If you want your Certificate Authority to sign the certificates that are generated upon deployment, skip to Step 5.
   - If you want to generate new certificates with custom options, such as a greater key size, continue to Step 3.
3. Run the command to back up the existing `certificates.ks` file.

   ```
   cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
   ```
4. Run the command to create public and private key pairs for the HTTPS service and for the console proxy service.

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool generate-certs -j -p -o /opt/vmware/
   vcloud-director/certificates.ks -w root_passwd
   ```

The command creates or updates a keystore at `certificates.ks`with the password that you specified. Certificates are created using the command's default values. Depending on the DNS configuration of your environment, the Issuer Common Name (CN) is set to either the IP address or the FQDN for each service. The certificate uses the default 2048-bit key length and expires one year after creation.

Important Because of configuration restrictions in vCloud Director appliance, you must use the location `/opt/vmware/vcloud-director/certificates.ks` for the certificates keystore.

Note You use the appliance **root** password as the keystore password.

5 Create certificate signing requests (CSR) for the HTTPS service and for the console proxy service.

Important The vCloud Director appliance shares the same IP address and hostname for both the HTTPS service and the console proxy service. Because of that, the CSR creation commands must have the same DNS and IPs for the Subject Alternative Name (SAN) extension argument.

a Create a certificate signing request in the `http.csr` file.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass root_password -certreq
-alias http -file http.csr -ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

b Create a certificate signing request in the `consoleproxy.csr` file.

```
keytool -keystore certificates.ks -storetype JCEKS -storepass
root_password -certreq -alias consoleproxy -file consoleproxy.csr -ext
"san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

6 Send the certificate signing requests to your Certificate Authority.

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

You obtain the CA-signed certificates.

7 Copy the CA-signed certificates, the CA root certificate, and any intermediate certificates to the vCloud Director appliance.

8 Run the commands to import the signed certificates into the JCEKS keystore.

a Import the Certificate Authority's root certificate from the `root.cer` file into the `certificates.ks` keystore file.

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias root -file root_certificate_file
```

b If you received intermediate certificates, import them from the `intermediate.cer` file to the `certificates.ks` keystore file.

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias intermediate -file intermediate_certificate_file
```

c Import the HTTPS service certificate.

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias http -file http_certificate_file
```

d Import the console proxy service certificate.

```
keytool -import -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -alias consoleproxy -file console_proxy_certificate_file
```

The commands overwrite the `certificates.ks` file with the newly acquired CA-signed versions of the certificates.

9 To check if the certificates are imported, run the command to list the contents of the keystore file.

```
keytool -storetype JCEKS -storepass root_password -keystore /opt/vmware/vcloud-director/certificates.ks -list
```

10 Run the command to import the certificates into the vCloud Director instance.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/vmware/vcloud-director/certificates.ks --keystore-password root_password
```

11 For the new signed certificates to take effect, restart the `vmware-vcd` service on the vCloud Director appliance.

```
service vmware-vcd restart
```

What to do next

- If you are using wildcard certificates, see Deploy the vCloud Director Appliance with Signed Wildcard Certificates for HTTPS and Console Proxy Communication .
- If you are not using wildcard certificates, repeat this procedure on all vCloud Director servers in the server group.

- For more information on replacing the certificates for the embedded PostgreSQL database and for the vCloud Director appliance management user interface, see Replace a Self-Signed Embedded PostgreSQL and vCloud Director Appliance Management UI Certificate.

Import Private Keys and CA-Signed SSL Certificates to the vCloud Director Appliance

If you have your own private key and CA-signed certificate files, before importing the keystores to your vCloud Director environment, you must create keystore files in which to import the certificates and the private keys for both the HTTPS and the console proxy service.

Prerequisites

- Familiarize yourself with the `keytool` command. You use `keytool` to import CA-signed SSL certificates to the vCloud Director appliance. vCloud Director places a copy of `keytool` at `/opt/vmware/vcloud-director/jre/bin/keytool`.
- Copy your intermediate certificates, root CA certificate, CA-signed HTTPS service and Console Proxy service private keys and certificates to the appliance.

Procedure

1. Log in directly or SSH to the vCloud Director appliance console as **root**.
2. If you have intermediate certificates, run the command to combine the root CA-signed certificate with the intermediate certificates and create a certificate chain.

   ```
   cat intermediate-certificate-file-1.cer intermediate-certificate-file-2.cer root-CA-certificate.cer > chain.crt
   ```

3. Use OpenSSL to create intermediate PKCS12 keystore files for both the HTTPS and the console proxy services with the private key, the certificate chain, the respective alias, and specify a password for each keystore file.
   a. Create the keystore file for the HTTPS service.

      ```
      openssl pkcs12 -export -in http.crt -inkey http.key -CAfile chain.crt -name http
      -passout pass:keystore_password -out http.pfx -chain
      ```

   b. Create the keystore file for the console proxy service.

      ```
      openssl pkcs12 -export -in consoleproxy.crt -inkey consoleproxy.key -CAfile chain.crt
      -name consoleproxy -passout pass:keystore_password -out consoleproxy.pfx -chain
      ```

4. Run the command to back up the existing `certificates.ks` file.

   ```
   cp /opt/vmware/vcloud-director/certificates.ks /root/certificates.ks.original
   ```

5 Use the `keytool` command to import the PKCS12 keystores into the JCEKS keystore.

   a Import the PKCS12 keystore for the HTTPS service.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/
vcloud-director/certificates.ks -deststoretype JCEKS -srckeystore http.pfx
-srcstoretype PKCS12 -srcstorepass keystore_password
```

   b Import the PKCS12 keystore for the console proxy service.

```
keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/
vcloud-director/certificates.ks -deststoretype JCEKS -srckeystore consoleproxy.pfx
-srcstoretype PKCS12 -srcstorepass keystore_password
```

6 Verify that the import of the certificates is successful.

```
keytool -storetype JCEKS -storepass keystore_password -keystore /opt/vmware/vcloud-
director/certificates.ks –list
```

7 Run the command to import the signed certificates into the vCloud Director instance.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
vmware/vcloud-director/certificates.ks --keystore-password keystore_password
```

8 For the CA-signed certificates to take effect, restart the `vmware-vcd` service on the vCloud Director appliance.

```
service vmware-vcd restart
```

What to do next

- If you are using wildcard certificates, see Deploy the vCloud Director Appliance with Signed Wildcard Certificates for HTTPS and Console Proxy Communication.
- If you are not using wildcard certificates, repeat this procedure on all vCloud Director appliance cells in the server group.
- For more information on replacing the certificates for the embedded PostgreSQL database and for the vCloud Director appliance management user interface, see Replace a Self-Signed Embedded PostgreSQL and vCloud Director Appliance Management UI Certificate.

Replace a Self-Signed Embedded PostgreSQL and vCloud Director Appliance Management UI Certificate

By default, the embedded PostgreSQL database and the vCloud Director appliance management user interface share a set of self-signed SSL certificates. For increased security, you can replace the default self-signed certificates with certificate authority (CA) signed certificates.

When you deploy the vCloud Director appliance, it generates self-signed certificates with a validity period of 365 days. The vCloud Director appliance uses two sets of SSL certificates. The vCloud Director service uses one set of certificates for HTTPS and the console proxy communications. The embedded PostgreSQL database and the vCloud Director appliance management user interface share the other set of SSL certificates.

Note The process of replacing the database and appliance management UI certificates does not affect the certificates for HTTPS and console proxy communications. Replacing one of the sets of certificates does not mean you must replace the other set.

Procedure

1. Send the certificate signing request which is located at `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` to the CA for signing.
2. If you are replacing the certificate for the primary database, place all other nodes into maintenance mode to prevent the possibility of data loss.
3. Replace the existing PEM-format certificate at `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` with the signed certificate, obtained from your CA in Step 1.
4. To pick up the new certificate, restart the vpostgres, nginx, and vcd_ova_ui services.

   ```
   systemctl restart nginx.service && systemctl restart vcd_ova_ui.service
   ```

   ```
   systemctl restart vpostgres.service
   ```

5. If you are replacing the certificate for the primary database, take all other nodes out of maintenance mode.

Results

The new certificate is imported to the vCloud Director truststore on other vCloud Director cells the next time the `appliance-sync` function runs. The operation might take up to 60 seconds.

Renew the vCloud Director Appliance Certificates

When you deploy the vCloud Director appliance, it generates self-signed certificates with a validity period of 365 days. If there are expiring or expired certificates in your environment, you can generate new self-signed certificates. You must renew the certificates for each vCloud Director cell individually.

The vCloud Director appliance uses two sets of SSL certificates. The vCloud Director service uses one set of certificates for HTTPS and console proxy communications. The embedded PostgreSQL database and the vCloud Director appliance management user interface share the other set of SSL certificates.

You can change both sets of self-signed certificates. Alternatively, if you use CA-signed certificates for the HTTPS and console proxy communications of vCloud Director, you can change only the embedded PostgreSQL database and appliance management UI certificate. CA-signed certificates include a complete trust chain rooted in a well-known public certificate authority.

Prerequisites

If you are renewing the certificate for the primary node in a database high availability cluster, place all other nodes in maintenance mode to prevent data loss. See Managing a Cell.

Procedure

1. Log in directly or SSH to the OS of the vCloud Director appliance as **root**.
2. To stop the vCloud Director services, run the following command.

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool -u administrator cell --shutdown
   ```

3. To generate new self-signed certificates, run the following command.

   ```
   /opt/vmware/appliance/bin/generate-certificates.sh <root-password>
   ```

   This command automatically puts into use the newly generated certificates for the embedded PostgreSQL database and the appliance management UI. The PostgreSQL and the Nginx servers restart. The command generates a new certificates keystore `/opt/vmware/vcloud-director/certificates.ks` with new self-signed certificates for the HTTPS and console proxy communication of vCloud Director, which are used in Step 4.
4. If you are not using CA-signed certificates, run the command to import the newly generated self-signed certificates to vCloud Director.

   ```
   /opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
   vmware/vcloud-director/certificates.ks --keystore-password <root-password>
   ```

5. Restart the vCloud Director service.

   ```
   service vmware-vcd start
   ```

Results

The renewed self-signed certificates are visible in the vCloud Director user interface.

The new PostgreSQL certificate is imported to the vCloud Director truststore on other vCloud Director cells the next time the `appliance-sync` function runs. The operation might take up to 60 seconds.

What to do next

If necessary, a self-signed certificate can be replaced with a certificate signed by an external or internal certificate authority.

vCloud Director Appliance Configuration

8

You can view the status of the cells in a database HA cluster, you can back up and restore the embedded database, you can reconfigure the appliance settings.

After you deploy the vCloud Director appliance, you cannot change the `eth0` and `eth1` network IP addresses or the hostname of the appliance. If you want the vCloud Director appliance to have different addresses or hostname, you must deploy a new appliance.

If you must perform maintenance of an appliance that requires shutting down the database high availability cluster, to avoid synchronization problems, you must first shut down the primary appliance and then the standby appliances.

This chapter includes the following topics:

View the Status of the Cells in a Database High Availability Cluster

To view the status of the primary and the standby cells in an appliance database high availability (HA) cluster, you can log in to the appliance management user interface of any cell from the database HA cluster.

The vCloud Director appliance database HA cluster consists of one primary and two standby cells. See Appliance Deployments and Database High Availability Configuration.

Procedure

1. In a Web browser, go to the appliance management user interface at `https://vcd_ip_address:5480`.
2. Log in as **root**.
3. To view the details about the cells in the database HA cluster, click **vCD Database Availability**.

Property	Description
Name	The DNS name of the cell.
Role	Can be either primary or standby. An appliance database HA cluster consists of one primary and two standby cells.
Status	Can be running, unreachable, or failed. An asterisk (*) indicates the status of the primary cell.
Following	The name of the primary cell with which the standby cell replicates.

What to do next

If a standby cell is not in a running state, deploy a new standby cell.

If the primary cell is not in a running state, Recover from a Primary Database Failure in a High Availability Cluster.

Recover from a Primary Database Failure in a High Availability Cluster

If the primary cell is not running properly, to recover the vCloud Director database, you can promote one of the standby cells to become the new primary cell. After that, you must deploy a new standby cell.

You can use this workflow to reuse the IP addresses and hostname of the failed primary when you deploy the new standby.

Prerequisites

- Verify that the primary cell is in the not reachable or failed state.
- Verify that the two standby cells are in the running state.
- Familiarize yourself with the procedure to remove a failed appliance from the vCloud Director server group and the repmgr high availability cluster. See Delete a Cloud Cell and Unregister a Failed Primary Cell in a Database High Availability Cluster .

See View the Status of the Cells in a Database High Availability Cluster.

Procedure

1 If possible, use the cell management tool to shut down the vCloud Director process. From the failed primary cell, run the following command.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

2 Power off the failed primary VM.

3 Log in as **root** to the appliance management user interface of a running standby cell, `https://standby_ip_address:5480`.

4 In the **Role** column for the standby cell that you want to become the new primary cell, click **Promote**.

The cell becomes the new primary cell in running state. The other standby cell is following the newly promoted primary cell.

5 Remove the failed primary appliance from both the vCloud Director server group and the repmgr high availability cluster.

6 If you want to reuse the IP address and hostname of the failed primary, ensure that the failed primary appliance remains powered off or delete it.

7 Deploy a new standby appliance. You can Start the vCloud Director Appliance Deployment or Deploying the vCloud Director Appliance by Using VMware OVF Tool.

After deploying the new standby appliance, the cluster health must be `Healthy`.

Important The OVA version of the newly deployed standby must be the same as the existing appliances in the cluster. To view the version of running appliances, see the About information in the appliance management UI. The appliance is distributed with a name of the form `VMware Cloud 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 Cloud Director-10.0.0.0-9229800_OVA10.ova.

Recover from a Standby Cell Failure in a High Availability Cluster

If a standby cell is not running properly, you can recover from the failure by deploying a new standby cell.

If one of the standby cells is in the `Unreachable` or `Failed` state, you can deploy a new cell. To view the state of the cells in the cluster, see View the Status of the Cells in a Database High Availability Cluster.

You can use this workflow to reuse the IP addresses and hostname of the failed standby when you deploy a new standby.

1 If possible, use the cell management tool to shut down the vCloud Director process. From the failed standby cell, run the following command.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

2 Power off the failed standby VM.

3 Remove the failed standby appliance from both the vCloud Director server group and the repmgr high availability cluster. See Delete a Cloud Cell and Unregister a Failed or Unreachable Standby Node in a Database High Availability Cluster.

4 If you want to reuse the IP address and DNS name of the failed standby cell, you must ensure that the failed standby remains powered off or delete it.

5 Deploy a new standby appliance. You can Start the vCloud Director Appliance Deployment or Deploying the vCloud Director Appliance by Using VMware OVF Tool.

After deploying the new standby, the cluster health must be `Healthy`.

Important The OVA version of the newly deployed standby must be the same as the existing appliances in the cluster. To view the version of running appliances, see the **About** information in the appliance management UI. The appliance is distributed with a name of the form `VMware Cloud 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 Cloud Director-10.2.0.0-9229800_OVA10.ova.

Embedded Database Backup and Restore of vCloud Director Appliance

You can back up the vCloud Director appliance embedded PostgreSQL database, which can help you to restore your vCloud Director environment after a failure.

Back up the vCloud Director Appliance Embedded Database

If your environment consists vCloud Director appliance deployments with embedded PostgreSQL databases, you can back up the vCloud Director database from the primary cell. The resulting `.tgz` file is stored on the NFS shared transfer service storage location.

Procedure

1 Log in directly or SSH to the primary cell as **root**.

2 Navigate to `/opt/vmware/appliance/bin`.

3 Run the `create-db-backup` command.

Results

On the NFS shared transfer service storage, in the *vcloudapp.nfs_mount.VMware_vCloud_Director*/pgdb-backup/ directory, you can see the newly created db-backup-*date_time_format*.tgz file. The .tgz file contains the database dump file, the global.properties, responses.properties, certificates, and proxycertificates files of the primary cell.

Restoring a vCloud Director Appliance Environment with a High Availability Database Configuration

If you backed up the embedded PostgreSQL database of a vCloud Director appliance environment with an HA database configuration, you can deploy a new appliance cluster and restore the appliance database in it.

To restore an appliance deployment with a non-HA database configuration, see Restoring a vCloud Director Appliance Environment Without a High Availability Database Configuration.

The restore workflow includes three major stages.

- Copying the embedded database backup .tar file from the transfer service NFS shared storage.
- Restoring the database to the embedded database primary and standby cells.
- Deploying any required application cells.

Prerequisites

- Verify that you have a backup .tar file of the embedded PostgreSQL database. See Back up the vCloud Director Appliance Embedded Database.
- Deploy one primary database cell and two standby database cells. See Chapter 6 Deploying the vCloud Director Appliance.
- If you want the new appliance cluster to use the NFS server of the previous environment, create and export a new directory on the NFS server as the new share. The existing mountpoint cannot be reused.

Procedure

1 On the primary and standby cells, log in as **root**, and run the command to stop the vCloud Director service.

```
service vmware-vcd stop
```

2 On the primary and standby cells, copy the backup .tar file to the /tmp folder.

If there is not enough free space on the /tmp folder, use another location to store the .tar file.

3 On the primary and standby cells, untar the backup file at `/tmp`.

```
tar -zxvf db-backup-date_time_format.tgz
```

In the `/tmp` folder, you can see the extracted `global.properties`, `responses.properties`, `certificates`, `proxycertficates`, `truststore`, and the database dump file named `vcloud_date_time_format`.

Note The `truststore` file is only available for vCloud Director 9.7.0.1 and later.

4 On the primary cell only, log in as **root** to the console and run the following commands.

a Drop the `vcloud` database.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

b Run the `pg_restore` command.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/
vcloud_date_time_name
```

5 On the primary and standby cells, save a copy of the configuration data files, replace them, and reconfigure and start the vCloud Director service.

a Back up the properties, certificates, and truststore files.

The `global.properties`, `responses.properties`, `certificates`, `proxycertificates`, and `truststore` files are at `/opt/vmware/vcloud-director/etc/`.

Note The `truststore` file is only available for vCloud Director 9.7.0.1 and later.

```
cd /opt/vmware/vcloud-director/etc
mkdir -p backup
cp global.properties responses.properties certificates proxycertificates truststore
backup
```

b Copy and replace the properties, certificates, and truststore files from the backup files that you extracted at Step 3.

```
cd /tmp
cp global.properties responses.properties certificates proxycertificates
truststore /opt/vmware/vcloud-director/etc/.
```

Note The `truststore` file is only available for vCloud Director 9.7.0.1 and later.

```
cp certificates /optvmware/vcloud-director/.
```

c Back up the keystore file that is at `/opt/vmware/vcloud-director/certificates.ks`.

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

d Run the command to reconfigure the vCloud Director service.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type
postgres --database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --
database-port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-
director/certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Where:

- The `--keystore-password` option matches the keystore password for the certificates on the appliance.
- The `--database-password` option matches the database password that you set during the appliance deployment.
- The `--database-host` option matches the `eth1` network IP address of the primary database appliance.
- The `--primary-ip` value matches the `eth0` network IP address of the appliance cell that you are restoring. This is not the primary database cell IP address.
- The `--console-proxy-ip` option matches the `eth0` network IP address of the appliance that you are restoring.

Note Do not run the reconfigure command on all cells at the same time.

For troubleshooting information, see Reconfiguring the vCloud Director Service Fails When Migrating or Restoring to vCloud Director Appliance.

e Run the command to start the vCloud Director service.

```
service vmware-vcd start
```

You can monitor the progress of the cell startup at `/opt/vmware/vcloud-director/logs/cell.log`.

6 (Optional) Deploy any additional application cells. See Chapter 6 Deploying the vCloud Director Appliance.

7 After all cells of the server group finish the startup process, verify that the restore of your vCloud Director environment is successful.

   a Open the vCloud Director Web Console by using the `eth0` network IP address of any cell from the new server group, `https://et0_IP_new_cell/cloud`.

   b Log in to the vCloud Director Web Console with your existing **system administrator** credentials.

   c Validate that your vSphere and cloud resources are available in the new environment.

8 After the successful verification of the database restore, use the vCloud Director Web Console to delete the disconnected cells that belong to the old vCloud Director environment.

   a From the **Manage & Monitor** tab, click **Cloud Cells**.

   b Right-click a cell name and select **Delete**.

Restoring a vCloud Director Appliance Environment Without a High Availability Database Configuration

If you backed up the embedded PostgreSQL database of a vCloud Director appliance environment with a non-HA database configuration, you can deploy a new appliance cluster and restore the appliance database in it.

To restore an appliance deployment with an HA database configuration, see Restoring a vCloud Director Appliance Environment with a High Availability Database Configuration.

The restore workflow includes three major stages.

- Copying the embedded database backup `.tar` file from the transfer service NFS shared storage.
- Restoring the database to the embedded database primary cell.
- Deploying any required application cells.

Prerequisites

- Verify that you have a backup `.tar` file of the embedded PostgreSQL database. See Back up the vCloud Director Appliance Embedded Database.
- Deploy one primary database cell. See Chapter 6 Deploying the vCloud Director Appliance.
- If you want the new appliance cluster to use the NFS server of the previous environment, create and export a new directory on the NFS server as the new share. The existing mountpoint cannot be reused.

Procedure

1 On the primary cell, log in as **root** to the console, and run the command to stop the vCloud Director service.

```
service vmware-vcd stop
```

2 Copy the backup `.tar` file to the `/tmp` folder.

   If there is not enough free space on the `/tmp` folder, use another location to store the `.tar` file.

3 Untar the backup file at `/tmp`.

```
tar -zxvf db-backup-date_time_format.tgz
```

   In the `/tmp` folder, you can see the extracted `global.properties`, `responses.properties`, `certificates`, `proxycertficates`, `truststore`, and the database dump file named `vcloud_date_time_format`.

   Note The `truststore` file is only available for vCloud Director 9.7.0.1 and later.

4 Run the commands to drop the database and restore it in the new appliance.

   a Drop the `vcloud` database.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

   b Run the `pg_restore` command.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/
vcloud_date_time_name
```

5 On the primary cell, save a copy of the configuration data files, replace them, and reconfigure and start the vCloud Director service.

   a Back up the properties, certificates, and truststore files.

   The `global.properties`, `responses.properties`, `certificates`, `proxycertificates`, and `truststore` files are at `/opt/vmware/vcloud-director/etc/`.

   Note The `truststore` file is only available for vCloud Director 9.7.0.1 and later.

```
cd /opt/vmware/vcloud-director/etc
mkdir -p backup
cp global.properties responses.properties certificates proxycertificates truststore
backup
```

b Copy and replace the properties, certificates, and truststore files from the backup files that you extracted at Step 3.

```
cd /tmp
cp global.properties responses.properties certificates proxycertificates
truststore /opt/vmware/vcloud-director/etc/.
```

Note The `truststore` file is only available for vCloud Director 9.7.0.1 and later.

```
cp certificates /optvmware/vcloud-director/.
```

c Back up the keystore file that is at `/opt/vmware/vcloud-director/certificates.ks`.

```
cd /opt/vmware/vcloud-director
mkdir -p backup
cp certificates.ks backup
```

d Run the command to reconfigure the vCloud Director service.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type
postgres --database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --
database-port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-
director/certificates.ks \
--keystore-password ks_password --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Where:

- The `--keystore-password` option matches the keystore password for the certificates on the appliance.
- The `--database-password` option matches the database password that you set during the appliance deployment.
- The `--database-host` option matches the `eth1` network IP address of the primary database appliance.
- The `--primary-ip` value matches the `eth0` network IP address of the appliance cell that you are restoring. This is not the primary database cell IP address.
- The `--console-proxy-ip` option matches the `eth0` network IP address of the appliance that you are restoring.

For troubleshooting information, see Reconfiguring the vCloud Director Service Fails When Migrating or Restoring to vCloud Director Appliance.

e Run the command to start the vCloud Director service.

```
service vmware-vcd start
```

You can monitor the progress of the cell startup at `/opt/vmware/vcloud-director/logs/cell.log`.

6 (Optional) Deploy any additional application cells. See Chapter 6 Deploying the vCloud Director Appliance.

7 After all cells of the server group finish the startup process, verify that the restore of your vCloud Director environment is successful.

   a Open the vCloud Director Web Console by using the `eth0` network IP address of any cell from the new server group, `https://et0_IP_new_cell/cloud`.

   b Log in to the vCloud Director Web Console with your existing **system administrator** credentials.

   c Validate that your vSphere and cloud resources are available in the new environment.

8 After the successful verification of the database restore, use the vCloud Director Web Console to delete the disconnected cells that belong to the old vCloud Director environment.

   a From the **Manage & Monitor** tab, click **Cloud Cells**.

   b Right-click a cell name and select **Delete**.

Configure External Access to the vCloud Director Database

You can enable access from particular external IP addresses to the vCloud Director database that is embedded in the primary appliance.

During a migration to the vCloud Director appliance, or if you plan to use a third party database backup solution, you might want to enable external access to the embedded vCloud Director database.

Procedure

1 Log in directly or SSH to the primary cell as **root**.

2 Navigate to the database directory, `/opt/vmware/appliance/etc/pg_hba.d/`.

3 Create a text file containing entries for the target external IP addresses similar to:

```
#TYPE  DATABASE  USER    ADDRESS        METHOD
host   vcloud    vcloud  CIDR_notation  md5
```

For example:

```
#TYPE  DATABASE  USER    ADDRESS           METHOD
host   vcloud    vcloud  172.168.100.5/32  md5
host   vcloud    vcloud  172.168.20.5/32   md5
```

Your entries are appended to the dynamically updated `pg_hba.conf` file, which controls the access to the primary database in the HA cluster.

Activate or Deactivate SSH Access to the vCloud Director Appliance

During the appliance deployment, you can leave deactivated or you can activate the SSH access to the appliance. After the deployment, you can switch the SSH access setting.

The SSH daemon runs in the appliance for use by the database HA function and for remote **root** logins. You can deactivate the SSH access for the **root** user. The SSH access for the database HA function remains unchanged.

Procedure

1 If you want to make temporary changes to the OVF property, for example, for testing purposes, change the property in vCloud Director.

   a Log in directly or by using an SSH client to the vCloud Director appliance console as **root**.

   b Run the script for activating or deactivating the SSH **root** access.

   - To activate the SSH **root** access, run the `/opt/vmware/appliance/bin/enable_root_login.sh` script.
   - To deactivate the SSH **root** access, run the `/opt/vmware/appliance/bin/disable_root_login.sh` script.

2 If you want to make permanent changes to the OVF property, use the vSphere user interface to set the value of the `vcloudapp.enable_ssh.VMware_vCloud_Director` property.

   Note You must power off the VM to change the value of the property in vSphere.

   - To activate SSH, set the value of `vcloudapp.enable_ssh.VMware_vCloud_Director` to **`True`**.
   - To deactivate SSH, set the value of `vcloudapp.enable_ssh.VMware_vCloud_Director` to **`False`**.

Edit the DNS Settings of the vCloud Director Appliance

After the deployment, you can change the DNS server or servers of the vCloud Director appliance.

Important You cannot edit the hostname of the appliance. You must deploy a new appliance with the desired hostname.

Procedure

1 If you want to change the DNS settings temporarily, for example, for testing purposes, edit the DNS settings in vCloud Director.

   a Log in directly or by using an SSH client to the vCloud Director appliance console as **root**.

   b (Optional) Verify the current DNS configuration by running the following command:

   ```
   ovfenv --key vami.DNS.VMware_vCloud_Director
   ```

   c Change the DNS server or servers.

   To specify multiple DNS servers set *DNS_server_IP* as a comma-separated list with no spaces.

   ```
   ovfenv --key vami.DNS.VMware_vCloud_Director --value DNS_server_IP
   ```

   d For the changes to take effect, restart the VAOS service.

   ```
   systemctl restart vaos.service
   ```

2 If you want to change the DNS settings permanently, use the vSphere UI to set the value of the `vami.DNS.VMware_vCloud_Director` property to the new DNS server IP address.

   To specify multiple DNS servers, enter a comma-separated list with no spaces.

   Note You must power off the VM to change the value of the property in vSphere.

Edit the Static Routes for the vCloud Director Appliance Network Interfaces

You can change the static routes for the `eth0` and `eth1` network interfaces after the initial vCloud Director deployment.

Procedure

1 If you want to change the static route value temporarily, for example, for testing purposes, edit the static routes in vCloud Director.

   a Log in directly or by using an SSH client to the vCloud Director appliance console as **root**.

   b (Optional) Verify the current static route configuration.

   - For `eth0`, run the following command.

     ```
     ovfenv --key vcloudnet.routes0.VMware_vCloud_Director
     ```

   - For `eth1`, run the following command.

     ```
     ovfenv --key vcloudnet.routes1.VMware_vCloud_Director
     ```

c Change the static route value.

The static routes must be in a comma-separated list of route specifications. For example, for `eth0` you must run:

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director  --value "172.16.100.253
172.16.96.0/19, 172.16.100.253 192.168.100.0/24"
```

- For `eth0`, run the following command.

```
ovfenv --key vcloudnet.routes0.VMware_vCloud_Director  --value "new_static_routes0"
```

- For `eth1`, run the following command.

```
ovfenv --key vcloudnet.routes1.VMware_vCloud_Director  --value "new_static_routes1"
```

d Restart the network service on the vCloud Director appliance.

```
systemctl restart vcd-ova-netconfig.service
```

2 If you want to change the static route value permanently, change the OVF property by using the vSphere UI.

The static routes must be in a comma-separated list of route specifications.

Note You must power off the VM to change the value of the property in vSphere.

- Use the vSphere user interface to set the value of the `vcloudnet.routes0.VMware_vCloud_Director` property to the new route specification string.
- Use the vSphere user interface to set the value of the `vcloudnet.routes1.VMware_vCloud_Director` property to the new route specification string.

Configuration Scripts in the vCloud Director Appliance

The vCloud Director appliance contains specific configuration scripts.

Directory	Description
`/opt/vmware/appliance/bin/`	The appliance configuration scripts.
`/opt/vmware/appliance/etc/`	The appliance configuration files.
`/opt/vmware/appliance/etc/pg_hba.d/`	The directory where you can add custom entries to the `pg_hba.conf` file. See Configure External Access to the vCloud Director Database.

Modify the PostgreSQL Configurations in the vCloud Director Appliance

You can change the vCloud Director appliance PostgreSQL configurations by using the PostgreSQL `ALTER SYSTEM` command.

The `ALTER SYSTEM` command writes the changes of the parameter settings to the `postgresql.auto.conf` file which takes precedence over the `postgresql.conf` file during the PostgreSQL initialization. Some settings require a restart of the PostgreSQL service while others are dynamically configured and do not require a restart. Do not change the `postgresql.conf` file, because those changes do not persist after reboot.

Procedure

1. Log in directly or by using an SSH client to the OS of the primary appliance as **root**.
2. Change the user to **postgres**.

   ```
   sudo -i -u postgres
   ```

3. Use the PostgreSQL `ALTER SYSTEM` command to change a parameter.

   ```
   psql -c "ALTER SYSTEM set parameter='value';"
   ```

4. Repeat Step 3 for each configuration parameter you want to change.
5. If some of the parameters you want to change require a restart of the PostgreSQL service, restart the vpostgres process.

   ```
   systemctl restart vpostgres
   ```

6. If your environment has standby nodes, copy the `postgresql.auto.conf` file to the standby appliances, and restart the PostgreSQL service if necessary.
   a. Copy the `postgresql.auto.conf` from the primary node to a standby node.

      ```
      scp /var/vmware/vpostgres/current/pgdata/postgresql.auto.conf postgres@<standby-node-address>:/var/vmware/vpostgres/current/pgdata/
      ```

   b. If some of the parameters in the copied `postgresql.auto.conf` file require a restart to take effect, restart the vpostgres process on the standby node.

      ```
      systemctl restart vpostgres
      ```

   c. Repeat 6.a and 6.b for each standby node.

Using the Replication Manager Tool Suite in a High Availability Cluster Configuration

9

The repmgr open-source tool suite is part of the embedded PostgreSQL database of the vCloud Director appliance. You can use repmgr to configure, monitor, and control PostgreSQL replication and database failover in your vCloud Director database high availability cluster.

You can use the repmgr command-line interface to check the status and events of a node or a cluster, to register or unregister a node, to promote a standby node, to swap the roles of a primary and a standby, or to follow a new primary node.

To learn more about vCloud Director database high availability configuration, see Appliance Deployments and Database High Availability Configuration.

To learn more about repmgr, visit repmgr.org.

This chapter includes the following topics:

Check the Connectivity Status of a Database High Availability Cluster

You can use the replication manager tool suite to check the connectivity between the nodes in your database high availability cluster.

Procedure

1 Log in or SSH as **`root`** to the OS of any of the running cells in the cluster.

2 Change the user to **postgres**.

```
sudo -i -u postgres
```

3 Check the connectivity of the cluster.

- The `repmgr cluster matrix` command runs the `repmgr cluster show` command on each node of the cluster and presents the result as a matrix.

  ```
  /opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/
  repmgr.conf cluster matrix
  ```

  In the following example, node 1 and node 2 are up, and node 3 is down. Each row corresponds to one server and represents the result of testing an outbound connection from that server.

  The three entries in the third row are marked with a `?` symbol because node 3 is down and there is no information on its outbound connections.

  ```
      Name| Id |  1 |  2  |  3
  ---------+----+----+----+----
    node 1 |  1 |  * |  * |  x
    node 2 |  2 |  * |  * |  x
    node 3 |  3 |  ? |  ? |  ?
  ```

- The `repmgr cluster crosscheck` command crosschecks the connections between each combination of nodes and might provide a better overview of the cluster connectivity.

  ```
  /opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/
  repmgr.conf cluster crosscheck
  ```

  In the following example, the node from which you run the `repmgr cluster crosscheck` command merges its cluster matrix system output with the output from the other nodes and does a crosscheck between the nodes. In this case, all nodes are up, but the firewall drops packets originating from node 1 and directed at node 3. This is an example of an asymmetric network partition, where node1 cannot send packets to node3.

  ```
      Name| Id |  1 |  2  |  3
  ---------+----+----+----+----
    node 1 |  1 |  * |  * |  x
    node 2 |  2 |  * |  * |  *
    node 3 |  3 |  * |  * |  *
  ```

What to do next

To determine the overall connectivity status in your database high availability cluster, run these commands on each node and compare the results.

Check the Replication Status of a Node in a Database High Availability Cluster

You can use the replication manager tool suite and the PostgreSQL interactive terminal to check the replication status of individual nodes in a database high availability cluster.

Procedure

1 Log in or SSH as **root** to the OS of any of the running nodes in the cluster.

2 Change the user to **postgres**.

```
sudo -i -u postgres
```

3 Check the replication status of the node.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf
node status
```

The system output provides information on the node, PostgreSQL version, and replication details.

4 (Optional) For more detailed information, use the PostgreSQL interactive terminal to check the replication status of the nodes.

The PostgreSQL interactive terminal can provide information regarding whether any of the received log records of the standby nodes are lagging behind the logs sent by the primary.

a Connect to the `psql` terminal

```
/opt/vmware/vpostgres/current/bin/psql
```

b To expand the display and make query results easier to read, run the `set \x` command.

c Run a replication status query depending on the role of the node.

Option	Action
Run a query on the primary node.	`/opt/vmware/vpostgres/current/bin/psql`
Run a query on a standby node.	`select * from pg_stat_wal_receiver;`

Check the Status of a Database High Availability Cluster

To troubleshoot problems in your database high availability cluster, you must monitor the status of the nodes and the events in the cluster.

Procedure

1 Log in or SSH as **root** to the OS of any of the running cells in the cluster.

2 Change the user to **postgres**.

```
sudo -i -u postgres
```

3 Check the status of the cluster.

The **Upstream** column shows the current primary node.

```
/opt/vmware/vpostgres/current/bin/repmgr cluster show
```

The console output displays the cluster information. In the following example, the primary node in the cluster, node 3, is unreachable.

```
     ID |  Name    | Role    | Status         | Upstream   | Location | Connection string
--------+----------+---------+----------------+------------+----------
+------------------------
 Node 1 | Node name | standby
|     running   | Node 3 name| default | host=host IP address user=repmgr dbname=repmgr
 Node 2 | Node name | standby
|     running   | Node 3 name| default | host=host IP address user=repmgr dbname=repmgr
 Node 3 | Node name | primary
| ? unreachable |            | default | host=host IP address user=repmgr dbname=repmgr
```

In the following system output example, node 3 is the primary node in a healthy running cluster.

```
     ID |  Name     | Role    | Status   | Upstream  | Location| Connection string
--------+-----------+---------+----------+-----------+---------+------------------------
 Node 1 | Node name | standby |  running | Node3 name| default | host=host IP address
user=repmgr dbname=repmgr
 Node 2 | Node name | standby |  running | Node3 name| default | host=host IP address
user=repmgr dbname=repmgr
 Node 3 | Node name | primary | *running |           | default | host=host IP address
user=repmgr dbname=repmgr
```

4 Check the cluster events log.

```
/opt/vmware/vpostgres/current/bin/repmgr -f /opt/vmware/vpostgres/current/etc/repmgr.conf
cluster event
```

The system output shows creation, cloning, and registration events in the cluster.

What to do next

If the status of the primary node is `unreachable` or `failed`, you must promote a standby node.

If the status of a standby node is `unreachable` or `failed`, repair the node and start the PostgreSQL service if it is not running.

Detecting a Former Primary Node That Comes Back Online in a High Availability Cluster

If a primary node in your cluster fails and then it comes back online when you promote a standby node to be the new primary, this causes inaccuracies in the repmgr data. You can detect irregularities with the `repmgr cluster show` command.

Example: Running `repmgr cluster show` on the Former Primary Node

In the following example, running the `repmgr cluster show` command on a former primary node that comes back online, results in the following system output.

```
     ID |  Name     | Role    | Status            | Upstream  | Location | Connection string
--------+-----------+---------+-------------------+-----------+----------
+------------------------
 Node 1 | Node1 name| standby |!
running as primary|Node 3 name| default  | host=host IP address user=repmgr dbname=repmgr
 Node 2 | Node2 name| standby |
running       |Node 3 name| default  | host=host IP address user=repmgr dbname=repmgr
 Node 3 | Node3 name| primary |
* running       |           | default  | host=host IP address user=repmgr dbname=repmgr
   WARNING: following issues were detected
  - node 1(ID: Node 1) is registered as standby but running as primary
```

In the example, node 1 is the current primary node in the cluster.

When you run the `repmgr cluster show` command, getting `!running as primary` status for a standby node indicates that a former primary node is running in the cluster. In this case, you must shut down and unregister the former primary node.

Example: Running `repmgr cluster show` on the New Primary

In the following example, running the `repmgr cluster show` command on the new primary node results in the following system output.

```
     ID |  Name    | Role    | Status     | Upstream   | Location | Connection string
--------+----------+---------+------------+------------+----------+------------------------
 Node 1 |Node1 name| primary |  * running |            | default  | host=host IP address
user=repmgr dbname=repmgr
 Node 2 |Node2 name| standby |    running | Node1 name | default  | host=host IP address
user=repmgr dbname=repmgr
 Node 3 |Node3 name| primary |  ! running |            | default  | host=host IP address
user=repmgr dbname=repmgr
   WARNING: following issues were detected
  - node 3(ID: Node 3) is running but the repmgr node record is inactive
```

In this case, the repmgr data is correct. It accurately indicates that node 1 is running and that it is the current primary node. The warning message about node 3, the former primary, indicates that the repmgr data on that node is not accurate.

Example: Running `repmgr cluster show` After Promoting a Standby Node, Without Running `standby follow` on the Remaining Standby Nodes

In the following example, you can see the repmgr data on each node in a cluster in which the primary node failed. A standby was promoted manually using the `repmgr standby promote` command, but without running `repmgr standby follow` on the remaining standby nodes.

When you run `repmgr cluster show` on the new primary, the system output represents correct repmgr data, but the new primary node, node 2, is not followed by any standby nodes.

```
     ID |  Name    | Role    | Status    | Upstream   |Location | Connection string
--------+----------+---------+-----------+------------+---------+-----------------------
 Node 1 |Node1 name| primary | * running |            | default | host=host IP address
user=repmgr dbname=repmgr
 Node 2 |Node2 name| primary | ! running |            | default | host=host IP address
user=repmgr dbname=repmgr
 Node 3 |Node3 name| standby |   running |Node 1 name | default | host=host IP address
user=repmgr dbname=repmgr
   WARNING: following issues were detected
  - node 1(ID: Node 1) is running but the repmgr node record is inactive
```

Both node 1, which is the former primary, and node 3, which is the standby that follows the former primary, provide inaccurate repmgr data.

```
     ID |  Name    | Role    | Status              | Upstream |Location | Connection string
--------+----------+---------+---------------------+----------+---------
+------------------------
 Node 1 |Node1 name| primary |
* running         |          | default | host=host IP address user=repmgr dbname=repmgr
 Node 2 |Node2 name| standby |!
running as primary |Node1 name| default | host=host IP address user=repmgr dbname=repmgr
 Node 3 |Node3 name| standby |
running         |Node1 name| default | host=host IP address user=repmgr dbname=repmgr
   WARNING: following issues were detected
  - node 2(ID: Node 2) is registered as standby but running as primary
```

Example: Running `repmgr cluster show` on a Standby Node

Running the command on a standby node that is following the current primary, results in a system output with accurate repmgr data that is identical to the data on the current primary.

Running the command on a standby node that is following the former primary, results in a system output with inaccurate repmgr data that is identical to the data on the former primary.

Log Entries

If a former primary that failed comes back online after you promote a standby node to be the new primary, the following entries appear in the `update-repmgr-data.log` file on all nodes with inaccurate repmgr data.

```
ERROR: An old primary is running in the repmgr cluster.
ERROR: Manual intervention is required to repair the repmgr cluster.
ERROR: The first step should be to shutdown and unregister the old primary.
```

Switch the Roles of the Primary and a Standby Cell in a Database High Availability Cluster

You can use a repmgr command to switch the roles of the primary and one of the standby nodes in your database high availability cluster during a planned maintenance.

Prerequisites

- Put all vCloud Director cells that are part of the high availability cluster into maintenance mode.
- Verify that all the nodes in the cluster are healthy and online.

Procedure

1. Log in or SSH as **`root`** to the OS of the standby node that you want to promote.
2. Change the user to **`postgres`**.

   ```
   sudo -i -u postgres
   ```

3. (Optional) Verify that the prerequisites for the switchover are met by running the command with the `--dry-run` option.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/
   current/etc/repmgr.conf --siblings-follow --dry-run
   ```

4. Switch the roles of the primary and the standby cell.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr standby switchover -f /opt/vmware/vpostgres/
   current/etc/repmgr.conf --siblings-follow
   ```

Results

The last line of the console output indicates that the standby switchover has completed successfully.

What to do next

1. Run the **`reconfigure-database`** command to update the database IP address on all vCloud Director cells. See Update the Database IP Addresses on vCloud Director Cells.

2 When you reconfigure the vCloud Director cells in the server group to point to the new primary database, take out of maintenance mode all vCloud Director cells that are part of the high availability cluster.

Unregister a Failed or Unreachable Standby Node in a Database High Availability Cluster

You can use repmgr on a running node on your cluster to unregister a failed or unreachable standby node.

Note For the primary node to function normally, at least one standby node must always be running.

Prerequisites

To unregister a standby node that is not running, you must provide the node ID. To find the IP address, check the status of the cluster and locate the node. On that row, use the host value from the Connection string column to identify the IP address of the node. See Check the Status of a Database High Availability Cluster.

Procedure

1 Log in or SSH as **`root`** to the OS of any of the running nodes of the cluster.

2 Change the user to **`postgres`**.

```
sudo -i -u postgres
```

3 Unregister the failed or unreachable node.

```
/opt/vmware/vpostgres/current/bin/repmgr standby unregister -f /opt/vmware/vpostgres/
current/etc/repmgr.conf --node-id=ID
```

Results

Unregistering the node removes the node information from the repmgr metadata.

Unregister a Failed Primary Cell in a Database High Availability Cluster

If the primary node in your database high availability cluster fails and you promote a new primary, you must unregister the failed primary node to remove it from the cluster and avoid inconsistent cluster status data.

Prerequisites

- To unregister a primary node that is not running, you must provide the node ID. To find the IP address, check the status of the cluster and locate the node. On that row, use the host value from the Connection string column to identify the IP address of the node. See Check the Status of a Database High Availability Cluster.
- Verify that the failed primary is inactive and without any following standby nodes, and promote a new primary.

Procedure

1. Log in or SSH as **`root`** to the OS of any of the running nodes in the cluster.
2. Change the user to **`postgres`**.

   ```
   sudo -i -u postgres
   ```

3. (Optional) To verify that the prerequisites for unregistering the node are met, run the command with the `--dry-run` option .

   ```
   /opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID --dry-run
   ```

4. Unregister the node.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=node ID
   ```

Results

The operation removes the node from the repmgr metadata.

Unregister a Running Standby Cell in a Database High Availability Cluster

If you want to use a node in another role, or if you want to remove it from the high availability cluster, you must unregister it.

You can run this command during the normal system operation.

Note For the primary node to function normally, at least one standby node must always be running.

Prerequisites

To unregister a standby node, you must provide the node ID. To find the IP address, check the status of the cluster and locate the node. On that row, use the host value from the Connection string column to identify the IP address of the node. See Check the Status of a Database High Availability Cluster.

Procedure

1. Log in or SSH as **root** to the OS of any of the running nodes in the cluster.
2. Change the user to **postgres**.

   ```
   sudo -i -u postgres
   ```

3. Unregister the node.

   ```
   /opt/vmware/vpostgres/current/bin/repmgr standby unregister --node-id=node ID -f /opt/
   vmware/vpostgres/current/etc/repmgr.conf
   ```

Results

Unregistering the node removes the record of the standby from the internal metadata table of the repmgr tool suite.

After you Install vCloud Director or Deploy the vCloud Director Appliance

10

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:

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 10-1. 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
```

Results

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.

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 5.

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 either the certificate uploaded to each vCloud Director cell keystore with alias **`HTTP`**, or, if SSL termination is used, the load balancer VIP certificate. 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 its `eth0` NIC with custom port 8443 for the console proxy service.

SSL termination of console proxy connections at a load balancer is not supported. The console proxy certificate is uploaded to each vCloud Director cell keystore with alias **`consoleproxy`**.

For example, for a vCloud Director appliance instance 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 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

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.

Perform Additional Configurations on the External PostgreSQL Database

After creating your vCloud Director server group, you can configure the external 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 external 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.

Upgrading vCloud Director and Patching the vCloud Director Appliance

11

You can perform an orchestrated upgrade, upgrade manually vCloud Director to a new version, or apply patches to the vCloud Director appliance deployments.

If your existing vCloud Director server group consists of vCloud Director installations on Linux, you can use the vCloud Director installer for Linux to upgrade your environment. As an alternative, you can migrate your environment to vCloud Director 9.7 appliance. See Chapter 12 Migrating to vCloud Director Appliance.

If your existing vCloud Director server group consists of vCloud Director 9.5 appliance deployments, you can only migrate your environment to vCloud Director 9.7 appliance. You use the vCloud Director installer for Linux to upgrade the existing environment only as part of the migration workflow. See Chapter 12 Migrating to vCloud Director Appliance.

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.
- Activating and deactivating ESXi hosts is unsupported. Before starting the upgrade, you must activate all ESXi hosts. You can put ESXi hosts in maintenance mode by using the vSphere Web Client.
- vCloud Director uses Java with an 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 13 After you Upgrade or Migrate 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, Configuration, 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.

Patching the vCloud Director Appliance Deployment

You can patch the vCloud Director appliance to improve its functionality or improve its security. See Patch the vCloud Director Appliance Deployment. After you apply the patch to every vCloud Director appliance and the database upgrade is complete, you must restart the vCloud Director services across the server group to bring it online again.

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
- Patch the vCloud Director Appliance Deployment

Perform an Orchestrated Upgrade of a vCloud Director Installation

You can upgrade all cells in the server group together with the shared database by running the vCloud Director installer with the `--private-key-path` option.

You can use the vCloud Director installer for Linux to upgrade a vCloud Director server group that consists of vCloud Director installations on a supported Linux OS. If your vCloud Director server group consists of vCloud Director 9.5 appliances deployments, you use the vCloud Director installer for Linux to upgrade your existing environment only as part of the migration workflow. See Chapter 12 Migrating to vCloud Director Appliance.

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 activated. Deactivated 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.

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.

Results

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 server group that consists of vCloud Director installations on a supported Linux OS. If your vCloud Director server group consists of vCloud Director 9.5 appliances deployments, you use the vCloud Director installer for Linux to upgrade your existing environment only as part of the migration workflow. See Chapter 12 Migrating to vCloud Director Appliance.

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 activated. Deactivated ESXi hosts are unsupported.

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.

Results

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.

Results

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 11-1. 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*.
`--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.

Table 11-1. Database Upgrade Utility Options and Arguments (continued)

Option	Argument	Description
`--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.

Patch the vCloud Director Appliance Deployment

You can update the vCloud Director appliance with patches that might be related to product functionality and security improvements.

During the patch of the vCloud Director appliance deployment, the vCloud Director service stops working and some downtime can be expected. The downtime depends on the time you need to patch each vCloud Director appliance and to run the vCloud Director database upgrade script. The number of working cells in the vCloud Director server group reduces until you stop the vCloud Director service on the last vCloud Director appliance. A properly configured load balancer in front of the vCloud Director HTTP endpoints should stop routing traffic to the cells that are stopped.

After you apply the patch to every vCloud Director appliance and the database upgrade is complete, you must restart the vCloud Director services across the server group to bring it online again.

Procedure

1. In a Web browser, log in to the appliance management user interface of a vCloud Director appliance instance to identify the primary appliance, `https://`*`appliance_ip_address`*`:5480`.

   Make a note of the primary appliance name. You must use the primary appliance name when upgrading the database.

2. Download the update package to an appliance.

   vCloud Director is distributed as an executable file with a name of the form `VMware_vCloud_Director_`*`v.v.v.v-nnnnnnnn`*`_update.tar.gz`, where *v.v.v.v* represents the product version and *nnnnnnnn* the build number. For example, `VMware_vCloud_Director_9.7.0.4248-13560441_update.tar.gz`.

3. Create the `local-update-package` directory in which to extract the update package.

   ```
   mkdir /tmp/local-update-package
   ```

4. Extract the update package in the newly created directory.

   ```
   tar -zxf VMware_vCloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz \
                  -C /tmp/local-update-package
   ```

5. Set the `local-update-package` directory as the update repository.

   ```
   vamicli    update --repo file:///tmp/local-update-package
   ```

6. Check for updates to verify that you established correctly the repository.

   ```
   vamicli update --check
   ```

   The patch release appears as an `Available Update`.

7 Shut down vCloud Director by running the following command:

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

8 From the primary appliance, back up the vCloud Director appliance embedded database.

Note If you are upgrading from vCloud Director 9.7.0.1 to a later version, manually back up the truststore file located at `/opt/vmware/vcloud-director/etc/truststore`.

```
/opt/vmware/appliance/bin/create-db-backup
```

9 Apply the available patch.

```
vamicli update --install latest
```

10 Repeat Step 2 to Step 7 and Step 9 on each appliance.

11 From any appliance, run the vCloud Director database upgrade script.

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

12 Start the vCloud Director services on each appliance.

```
service vmware-vcd start
```

Migrating to vCloud Director Appliance

12

Starting with version 9.7, the vCloud Director appliance includes an embedded PostgreSQL database with a high availability function. You can migrate your existing vCloud Director environment of an earlier version to a vCloud Director environment that consists of vCloud Director 9.7 appliance deployments.

You can migrate a vCloud Director environment that consists of vCloud Director installations on Linux or vCloud Director appliance deployments. You can migrate a vCloud Director environment that uses an external Microsoft SQL database or an external PostgreSQL database.

If your vCloud Director environment uses an external Oracle database, before migrating to vCloud Director appliance, you must migrate the database to PostgreSQL from vCloud Director version 9.1. For information about the workflow for upgrading a vCloud Director installation with an Oracle Database, see Chapter 11 Upgrading vCloud Director and Patching the vCloud Director Appliance.

This chapter includes the following topics:

Migrating vCloud Director with an External Microsoft SQL Database to vCloud Director Appliance

If your current vCloud Director environment of an earlier version uses an external Microsoft SQL database, you can migrate to a new vCloud Director environment that consists of vCloud Director 9.7 appliance deployments. Your current vCloud Director environment can consist of vCloud Director installations on Linux or vCloud Director appliance deployments. The new vCloud Director environment can use the appliance embedded PostgreSQL databases in a high availability mode.

The migration workflow includes four major stages.

- Creating the new vCloud Director server group by deploying one or more instances of the vCloud Director 9.7 appliance
- Upgrading the existing vCloud Director environment
- Migrating the external to the embedded database
- Copying the shared transfer service data and the certificates data.

Procedure

1 Upgrade your current vCloud Director environment to version 9.7, and upgrade the source database schema.

   See Chapter 11 Upgrading vCloud Director and Patching the vCloud Director Appliance.

2 Verify that the migration source vCloud Director restart is successful.

3 If you want the new vCloud Director environment to use the IP addresses of the existing environment, change the IP addresses of the existing cells to temporary IP addresses.

4 If you want the new vCloud Director environment to use the NFS server of the existing environment, create and export a new directory on this NFS server as the new shared NFS mountpoint.

   You cannot reuse the existing mountpoint because the user and group IDs (UID/GID) of the users in the old NFS might not match the user and group IDs in the new NFS.

5 Create the new server group by deploying one or more instances of the vCloud Director 9.7 appliance.

   - If you want to use the database high availability function, deploy one primary and two standby cells, and, optionally, one or more vCD application cells.
   - If you changed the IP addresses of the existing cells to temporary IP addresses, you can use the original IP addresses for the new cells.
   - If you exported a new path on the existing NFS server, you can use this new shared mountpoint for the new environment.

   See Chapter 6 Deploying the vCloud Director Appliance.

6 On each existing cell and on each newly deployed cell, run the command to stop the vCloud Director service.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

7 Choose one of the existing cells to serve as a migration source.

   The migration source must have access to the `eth1` network IP address of the newly deployed primary cell.

8 On the new primary cell, enable access to the embedded database from the migration source.

   See Configure External Access to the vCloud Director Database.

9 On the migration source, run the cell management tool to migrate the external database to the database that is embedded in the new primary cell.

   The embedded database uses the `eth1` network IP address of the appliance.

```
/opt/vmware/vcloud-director/bin/cell-management-tool dbmigrate -dbhost eth1_IP_new_primary
\
-dbport 5432 -dbuser vcloud -dbname vcloud -dbpassword database_password_new_primary
```

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

10 On each newly deployed cell, back up and replace the configuration data, and reconfigure and start the vCloud Director service.

a Back up the properties and the certificates files, and copy and replace these files from the migration source.

The `global.properties`, `responses.properties`, `certificates`, and `proxycertificates` files are at `/opt/vmware/vcloud-director/etc/`.

Important If you are migrating to vCloud Director version 9.7.0.1 or later, you must also back up, copy, and replace the `truststore` file from the migration source, along with the other files.

b Back up the keystore file that is at `/opt/vmware/vcloud-director/certificates.ks`.

Do not copy and replace with the keystore file from the migration source.

c Run the command to reconfigure the vCloud Director service.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type
postgres --database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --
database-port 5432 \
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-
director/certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Where:

- The `--keystore-password` value matches the initial **root** password of this appliance.
- The `--database-password` value matches the database password that you set during the appliance deployment.
- The `--database-host` value matches the `eth1` network IP address of the primary appliance.
- The `--keystore` value is the path to the `certificates.ks` file you backed up in Step 10.b.
- The `--primary-ip` value matches the `eth0` network IP address of the appliance.
- The `--console-proxy-ip` value matches the `eth0` network IP address of the appliance.

For troubleshooting information, see Reconfiguring the vCloud Director Service Fails When Migrating or Restoring to vCloud Director Appliance.

d Run the command to start the vCloud Director service.

```
service vmware-vcd start
```

You can monitor the progress of the cell startup at `/opt/vmware/vcloud-director/logs/cell.log`.

11 After all cells of the new server group finish the startup process, verify that the migration of your vCloud Director environment is successful.

   a Open the vCloud Director Web Console by using the `eth0` network IP address of any cell from the new server group, `https://et0_IP_new_cell/cloud`.

   b Log in to the vCloud Director Web Console with your existing **system administrator** credentials.

   c Validate that your vSphere and cloud resources are available in the new environment.

12 After the successful verification of the vCloud Director migration, use the vCloud Director Web Console to delete the disconnected cells that belong to the old vCloud Director environment.

   a From the **Manage & Monitor** tab, click **Cloud Cells**.

   b Right-click a cell name and select **Delete**.

You can deploy the vCloud Director appliance to add members to the server group of the migrated environment.

What to do next

The new migrated vCloud Director appliance environment uses self-signed certificates. To use the well-signed certificates from the old environment, on each cell of the new environment, follow these steps:

1 Copy and replace the keystore file from the old cell to `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.

2 Run the cell management tool command to replace the certificates.

   Ensure that `vcloud.vcloud` is the owner of this file.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
vmware/vcloud-director/data/transfer/certificates.ks \
--keystore-password ks_password_old_vCD
```

3 Restart the vCloud Director service.

```
service vmware-vcd restart
```

If you add new members to this server group, the new appliance cells are deployed with these well-signed certificates.

Migrating vCloud Director with an External PostgreSQL Database to vCloud Director Appliance

If your current vCloud Director environment of an earlier version uses an external PostgreSQL database, you can migrate to a new vCloud Director environment that consists of vCloud Director 9.7 appliance deployments. Your current vCloud Director environment can consist of vCloud Director installations on Linux or vCloud Director appliance deployments. The new vCloud Director environment can use the appliance embedded PostgreSQL databases in a high availability mode.

The migration workflow includes four major stages.

- Upgrading the existing vCloud Director environment
- Creating the new vCloud Director server group by deploying one or more instances of the vCloud Director 9.7 appliance
- Migrating the external to the embedded database
- Copying the shared transfer service data and the certificates data.

Procedure

1 If your current external PostgreSQL database is of version 9.x, upgrade the external PostgreSQL database to version 10.

2 Upgrade your current vCloud Director environment to version 9.7.

See Chapter 11 Upgrading vCloud Director and Patching the vCloud Director Appliance.

3 Verify that the migration source vCloud Director restart is successful.

4 On each cell of the upgraded vCloud Director environment, run the command to stop the vCloud Director service.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <admin username> cell --shutdown
```

5 On the external PostgreSQL database, back up the current database.

```
sudo -u postgres path_to_pg_dump -Fc db_name > /tmp/db_dump_name
```

If there is not enough free space on the `/tmp` folder, use another location to store the dump file.

6 If the database owner and database name are different from `vcloud`, make a note of the user name and database name.

You must create this user in the new environment and rename the database at Step 13.

7 If you want the new vCloud Director environment to use the IP addresses of the existing environment, you must copy the properties and the certificates files to a location on the external PostgreSQL database and power off the cells.

   a Copy the `global.properties`, `responses.properties`, `certificates`, and `proxycertificates` files located at `/opt/vmware/vcloud-director/etc/` to the `/tmp` or any preferred location on the external PostgreSQL database.

   b Power off the cells in the existing environment.

8 If you want the new vCloud Director environment to use the NFS server of the existing environment, create and export a new directory on this NFS server as the new shared NFS mountpoint.

   You cannot reuse the existing mountpoint because the user and group IDs (UID/GID) of the users in the old NFS might not match the user and group IDs in the new NFS.

9 Create the new server group by deploying one or more instances of the vCloud Director 9.7 appliance.

   - If you want to use the database high availability function, deploy one primary and two standby cells, and, optionally, one or more vCD application cells.
   - If you powered off the cells in the existing environment, you can use the original IP addresses for the new cells.
   - If you exported a new path on the existing NFS server, you can use this new shared mountpoint for the new environment.

   See Chapter 6 Deploying the vCloud Director Appliance.

10 On each newly deployed cell, run the command to stop the vCloud Director service.

```
service vmware-vcd stop
```

11 Copy the dump file from the `/tmp` folder on the external PostgreSQL database to the `/tmp` folder on the primary cell of the new environment.

   See Step 5.

12 Change the permissions on the dump file.

```
chmod a+r /tmp/db_dump_name
```

13 Log in as **root** to the console of the newly deployed primary cell, and transfer the vCloud Director database from the external to the embedded database.

   a Switch the user to `postgres`, connect to the `psql` database terminal, and run the statement to drop the `vcloud` database.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'DROP DATABASE vcloud;'
```

b If the database owner of the existing external database is different from `vcloud`, create a user with the name that you noted at Step 6.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'CREATE USER
<db_owner_external_pg>;'
```

c Run the `pg_restore` command.

```
sudo -u postgres /opt/vmware/vpostgres/current/bin/pg_restore -C -d postgres /tmp/
db_dump_name
```

d If the database name of the existing external database is different from `vcloud`, change the database name to `vcloud` by using the name that you noted at Step 6.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE
<db_name_external_pg> RENAME TO vcloud;'
```

e If the database owner of the existing vCloud Director environment is different from `vcloud`, change the database owner to `vcloud`, and reassign the tables to `vcloud`.

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -c 'ALTER DATABASE vcloud
OWNER TO vcloud;'
```

```
sudo -i -u postgres /opt/vmware/vpostgres/current/bin/psql -d vcloud -c 'REASSIGN
OWNED BY <db_owner_external_pg> TO vcloud;'
```

14 On each newly deployed cell, back up and replace the configuration data, and reconfigure and start the vCloud Director service.

a Back up the properties and the certificates files, and copy and replace these files from the location on the external PostgreSQL database of the migration source, to which you copied the files in step 7a.

The `global.properties`, `responses.properties`, `certificates`, and `proxycertificates` files are at `/opt/vmware/vcloud-director/etc/`.

Important If you are migrating to vCloud Director version 9.7.0.1 or later, you must also back up, copy, and replace the `truststore` file from the migration source, along with the other files.

b Back up the keystore file that is at `/opt/vmware/vcloud-director/certificates.ks`.

Do not copy and replace with the keystore file from the migration source.

c Run the command to reconfigure the vCloud Director service.

```
/opt/vmware/vcloud-director/bin/configure --unattended-installation --database-type
postgres --database-user vcloud \
--database-password db_password_new_primary --database-host eth1_ip_new_primary --
database-port 5432 \
```

```
--database-name vcloud --database-ssl true --uuid --keystore /opt/vmware/vcloud-
director/certificates.ks \
--keystore-password root_password_new_primary --primary-ip appliance_eth0_ip \
--console-proxy-ip appliance_eth0_ip --console-proxy-port-https 8443
```

Where:

- The `--keystore-password` value matches the initial **root** password of this appliance.
- The `--database-password` value matches the database password that you set during the appliance deployment.
- The `--database-host` value matches the `eth1` network IP address of the primary appliance.
- The `--primary-ip` value matches the `eth0` network IP address of the appliance.
- The `--console-proxy-ip` value matches the `eth0` network IP address of the appliance.
- The `--console-proxy-port` value matches the appliance console proxy port 8443.

For troubleshooting information, see Reconfiguring the vCloud Director Service Fails When Migrating or Restoring to vCloud Director Appliance.

d Run the command to start the vCloud Director service.

```
service vmware-vcd start
```

You can monitor the progress of the cell startup at `/opt/vmware/vcloud-director/logs/cell.log`.

15 After all cells of the new server group finish the startup process, verify that the migration of your vCloud Director environment is successful.

a Open the vCloud Director Web Console by using the `eth0` network IP address of any cell from the new server group, `https://et0_IP_new_cell/cloud`.

b Log in to the vCloud Director Web Console with your existing **system administrator** credentials.

c Validate that your vSphere and cloud resources are available in the new environment.

16 After the successful verification of the vCloud Director migration, use the vCloud Director Web Console to delete the disconnected cells that belong to the old vCloud Director environment.

a From the **Manage & Monitor** tab, click **Cloud Cells**.

b Right-click a cell name and select **Delete**.

You can deploy the vCloud Director appliance to add members to the server group of the migrated environment.

What to do next

The new migrated vCloud Director appliance environment uses self-signed certificates. To use the well-signed certificates from the old environment, on each cell of the new environment, follow these steps:

1 Copy and replace the keystore file from the old cell to `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.

2 Run the cell management tool command to replace the certificates.

Ensure that `vcloud.vcloud` is the owner of this file.

```
/opt/vmware/vcloud-director/bin/cell-management-tool certificates -j -p --keystore /opt/
vmware/vcloud-director/data/transfer/certificates.ks \
--keystore-password ks_password_old_vCD
```

3 Restart the vCloud Director service.

```
service vmware-vcd restart
```

If you add new members to this server group, the new appliance cells are deployed with these well-signed certificates.

After you Upgrade or Migrate vCloud Director

13

After you upgraded or migrated 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.

Important Starting with version 9.7, vCloud Director supports only advanced edge gateways. You must convert any legacy non-advanced edge gateway to an advanced gateway. See https://kb.vmware.com/kb/66767.

This chapter includes the following topics:

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. Deactivate 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.

New Rights in This Release

vCloud Director 9.7 introduces new rights, which you might want to add to any existing global roles that you published to your tenants.

Right	Description	Default Role
SDDC: View SDDC	Allows you to view all SDDCs that are published to your organization. The **system administrator** can view all SDDCs.	**System Administrator** and **Organization Administrator**
SDDC: Manage SDDC	Allows you to add, remove, and edit SDDCs.	**System Administrator**
SDDC: Manage SDDC Proxy	Allows you to add, remove, activate, and deactivate SDDC proxies.	**System Administrator**
Service Applications: View Service Applications	Allows you to see the list of registered service applications. Used for VMC accounts.	**System Administrator**
Service Applications: Register VMC SDDC	Allows you to create, view, edit, and remove service applications. Used for VMC accounts.	**System Administrator**
Service Applications: Manage Service Applications	Allows you to register service applications. Used for VMC accounts.	**System Administrator**
Edge Cluster: View Edge Cluster	Allows you to see a list of edge cluster, and to retrieve an individual edge cluster.	**System Administrator** and **Organization Administrator**
Edge Cluster: Manage Edge Cluster	Allows you to create, edit, and remove edge clusters.	**System Administrator** and **Organization Administrator**
vApp: Edit VM Compute Policy	Allows users to change the compute policy of a virtual machine.	**system administrator**, **organization administrator**, **Catalog Author**, and **vApp Author**
Gateway: Import Edge Gateway	Allows you to import a Tier-1 router as an edge gateway.	**System Administrator** and **Organization Administrator**

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

Troubleshooting the vCloud Director Appliance

14

If the vCloud Director appliance deployment fails or if the appliance is not operating properly, you can examine the appliance log files to determine the cause of the problem.

VMware Technical Support routinely requests diagnostic information handling support requests. You can use the `vmware-vcd-support` script to collect host log information, and vCloud Director logs. For more information about collecting diagnostic information for vCloud Director, see https://kb.vmware.com/s/article/1026312. When running the `vmware-vcd-support` script, the logs might include information about decommissioned or replaced cells with status `FAIL`. See, https://kb.vmware.com/s/article/71349.

This chapter includes the following topics:

Examine the Log Files in the vCloud Director Appliance

After you deploy the vCloud Director appliance, you can examine the firstboot and database logs for errors and warnings.

Procedure

1. Log in directly or SSH to the vCloud Director appliance console as **root**.
2. Navigate to `/opt/vmware/var/log`.
3. Examine the log files.
   - The `firstboot` file contains logging information related to the first boot of the appliance.
   - The `/opt/vmware/var/log/vcd/` directory contains logs related to the Replication Manager (repmgr) tool suite setup and reconfiguration and appliance synchronization.

- The `/opt/vmware/var/log/vcd/pg/` directory contains logs related to the backup of the embedded appliance database.
- The `/opt/vmware/etc/vami/ovfEnv.xml` file contains the deployment OVF parameters.

The vCloud Director Cell Fails to Start After the Appliance Deployment

You deployed the vCloud Director appliance successfully, but the vCloud Director services might fail to start.

Problem

The `vmware-vcd` service is inactive after the appliance deployment.

Cause

If you deployed a primary cell, the vCloud Director services might fail to start due to a pre-populated NFS shared transfer service storage. Before you deploy the primary appliance, the shared transfer service storage must not contain a `responses.properties` file or an `appliance-nodes` directory.

If you deployed a standby or vCD application cell, the vCloud Director services might fail to start due to a missing `responses.properties` file in the NFS shared transfer storage. Before you deploy a standby or vCD application appliance, the shared transfer service storage must contain the `responses.properties` file.

Solution

1. Log in directly or SSH to the vCloud Director appliance console as **root**.
2. Examine the `/opt/vmware/var/log/vcd/setupvcd.log` for error messages regarding the NFS storage.
3. Prepare the NFS storage for the appliance type.
4. Redeploy the cell .

Reconfiguring the vCloud Director Service Fails When Migrating or Restoring to vCloud Director Appliance

When you are migrating or restoring to vCloud Director appliance, running the `configure` command might fail.

Problem

During the procedure for migrating or restoring vCloud Director to a new vCloud Director appliance environment, you run the `configure` command to reconfigure the vCloud Director service in each new cell. The `configure` command might fail with the error message `sun.security.validator.ValidatorException: PKIX path validation failed: java.security.cert.CertPathValidatorException: signature check failed`.

Solution

1 On the target cell, run the command.

```
sed -i '/vcd_ova.crt/ s/$/ --force /' /opt/vmware/appliance/bin/appliance-sync.sh
```

2 Wait 1 minute, and rerun the `configure` command.

Using the Log Files to Troubleshoot vCloud Director Updates and Patches

You can examine the log files for errors and warnings when you apply patches to the vCloud Director appliance.

Problem

If the `vamicli` command returns an error, you can use the log files to troubleshoot.

Solution

1 Log in directly or SSH to the vCloud Director appliance console as **root**.

2 Navigate to the appropriate log file.

- If the `vamicli update --check` fails, navigate to `/opt/vmware/var/log/vami/vami.log`.
- If the `vamicli update --install latest` fails, navigate to `/opt/vmware/var/log/vami/updatecli.log`.

3 Examine the log file.

Checking for vCloud Director Updates Fails

When you are checking for updates to the vCloud Director appliance, running the `vamicli update --check` command might fail.

Problem

During the procedure of applying a patch to the vCloud Director appliance, you run the `vamicli update --check` command to check for available updates. The `vamicli update --check` command might fail with `Failure: Error downloading manifest. Please contact your vendor.`

Cause

The path to the update repository directory is incorrect.

Solution

1 Run the `vamicli` command with the correct path.

```
vamicli update --repo file:/root/local-update-repo
```

2 Run again the command to check for updates.

```
vamicli update --check
```

Installing the Latest Update of vCloud Director Fails

When you are installing the latest updates to the vCloud Director appliance, running the `vamicli update --install latest` command might fail.

Problem

During the procedure of applying a patch to the vCloud Director appliance, you run the `vamicli update --install latest` command to apply the latest available patch. The `vamicli update --install latest` command might fail with `Failure: Error while running package installation`

Cause

The error occurs when the NFS server is inaccessible.

Solution

1 Verify that the NFS server mounted at `/opt/vmware/vcloud-director/data/transfer` is accessible.

2 Run again the command to apply the available patch.

```
vamicli update --install latest
```

Uninstall vCloud Director Software

15

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.