VMware Cloud Director Installation, Configuration, and Upgrade Guide

Modified on 8 APR 2021
VMware Cloud Director 10.2

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

VMware Cloud Director™ Installation, Configuration, and Upgrade Guide

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

Intended Audience

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

VMware Cloud Director Architecture

1

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

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

To ensure VMware Cloud Director high availability, you must install at least two VMware Cloud 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 VMware Cloud Director installation to multiple VMware vCenter Server® systems and the VMware ESXi™ hosts that they manage. For network services, VMware Cloud Director can use NSX Data Center for vSphere associated with vCenter Server or you can register NSX-T Data Center with VMware Cloud Director. Mixed NSX Data Center for vSphere and NSX-T Data Center are also supported.

Figure 1-1. VMware Cloud Director Linux Installation Architecture Diagram

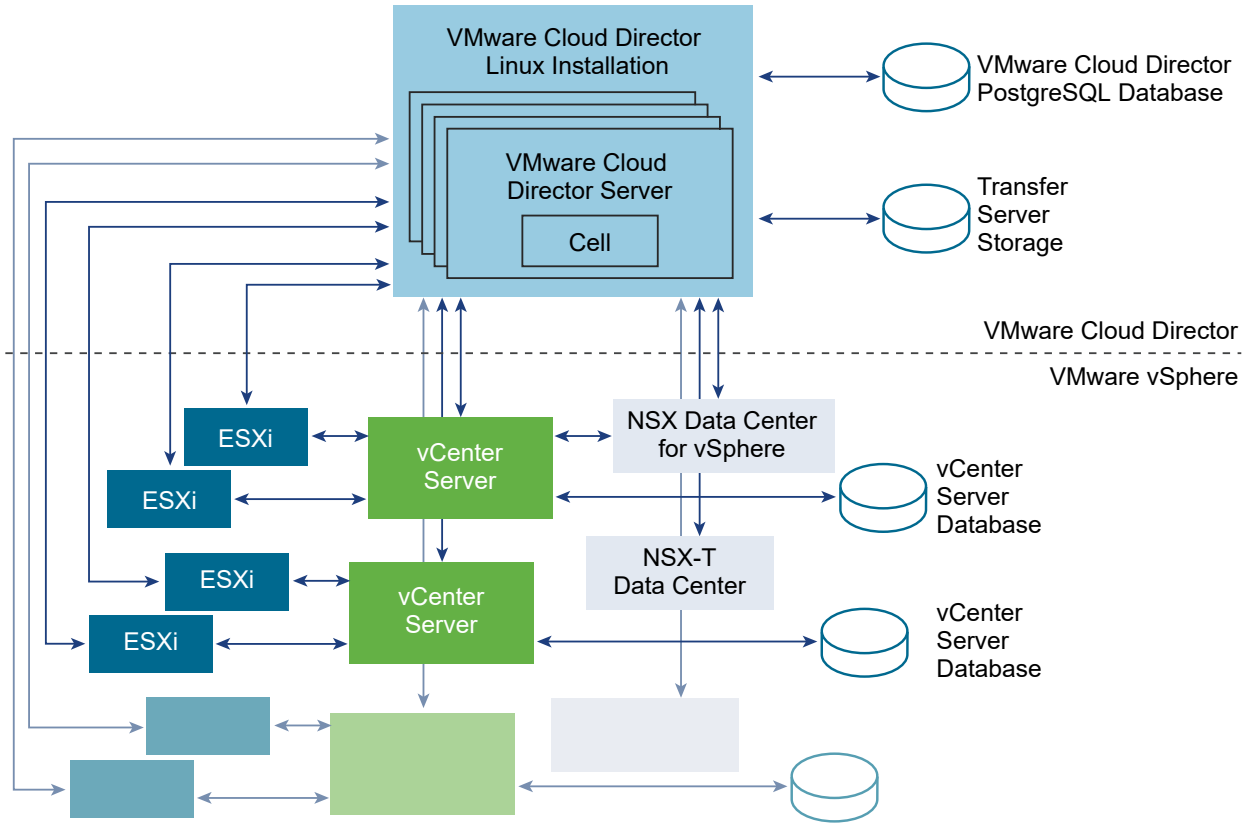
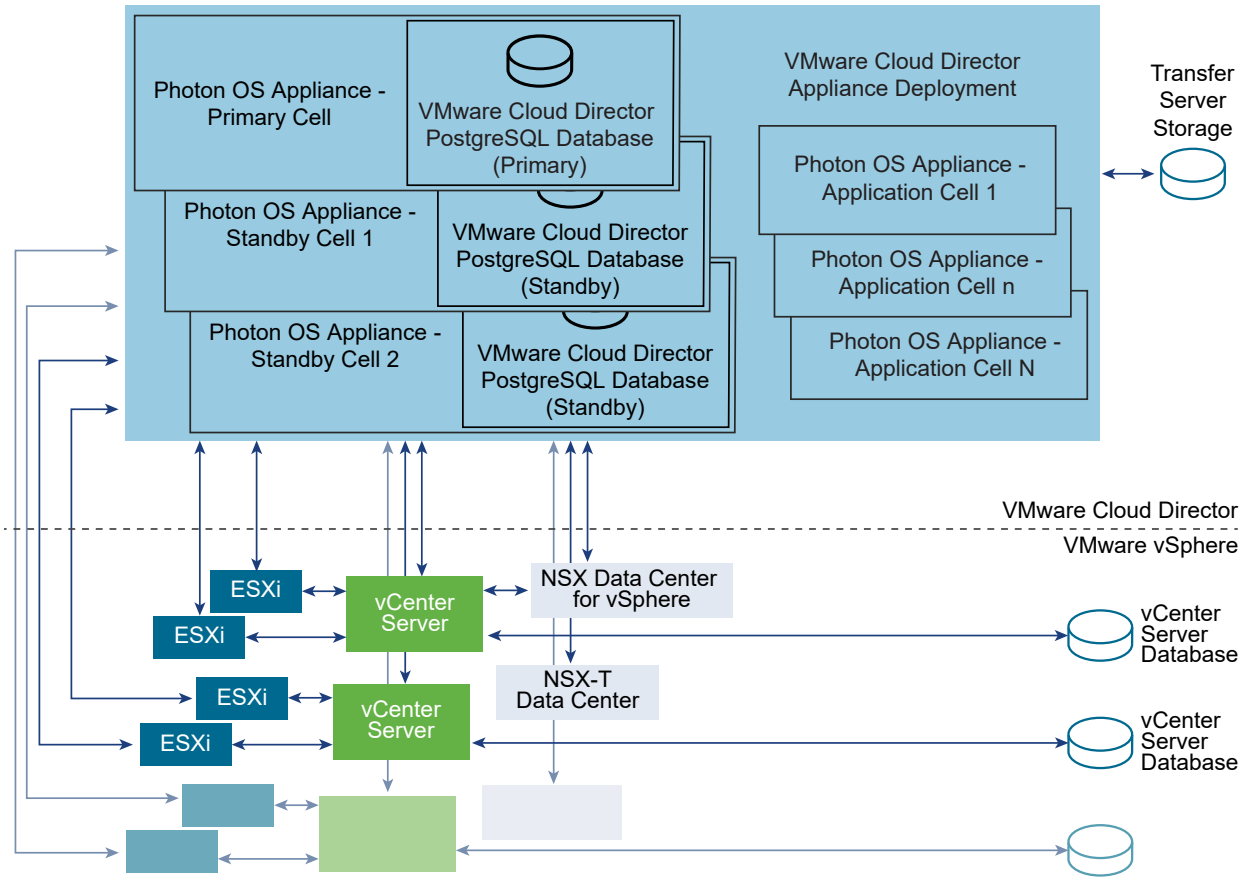


Figure 1-2. VMware Cloud Director Appliance Architecture Diagram



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

A VMware Cloud Director server group that consists of appliance deployments uses the embedded database in the first member of the server group. You can configure a VMware Cloud 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 1-3. VMware Cloud Director Appliances Comprising an Embedded Database High Availability Cluster

The VMware Cloud 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 or NSX-T Manager instances.

For information about adding vSphere and network resources, see the *VMware Cloud Director Service Provider Admin Portal Guide*.

VMware Cloud Director Hardware and Software Requirements

2

Each server in a VMware Cloud 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 VMware Cloud 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 VMware Cloud Director must meet specific configuration requirements.

- vCenter Server networks intended for use as VMware Cloud Director external networks or network pools must be available to all hosts in any cluster intended for VMware Cloud Director to use. Making these networks available to all hosts in a data center simplifies the task of adding new vCenter Server instances to VMware Cloud Director.
- vSphere Distributed Switches are required for isolated networks and network pools backed by NSX Data Center for vSphere.
- vCenter Server clusters used with VMware Cloud 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 VMware Cloud 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.

Supported Platforms, Databases, and Browsers

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

Disk Space, Memory, and CPU Requirements

For more information about disk space, memory, and CPU requirements, see VMware Cloud Director Appliance Sizing Guidelines.

Shared Storage

NFS or other shared storage volume for the VMware Cloud 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 VMware Cloud Director

Secure, reliable operation of VMware Cloud 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 VMware Cloud Director.

The network that connects the VMware Cloud Director servers, the database server, the vCenter Server systems, and the NSX components, must meet several requirements:

IP addresses

Each VMware Cloud Director server must support two different SSL endpoints. One endpoint is for the HTTPS 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 VMware Cloud 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 Service Provider Admin Portal. For example, for the VMware Cloud 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 VMware Cloud Director servers, including the database server. The maximum allowable drift between the clocks of synchronized servers is 2 seconds.

For the VMware Cloud Director appliance deployments, the NFS server used for the transfer share must use a network time service such as NTP to synchronize its clock with that of the VMware Cloud Director appliances. The maximum allowable drift between the clocks of synchronized servers is 2 seconds.

Server Time Zones

All VMware Cloud Director servers, including the NFS server used for the transfer share and 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 VMware Cloud 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 VMware Cloud Director requires a secure network environment. Configure and test this network environment before you begin installing VMware Cloud Director.

Connect all VMware Cloud Director servers to a network that is secured and monitored.

For information on the network ports and protocols used by VMware Cloud Director, see VMware Ports and Protocols.

VMware Cloud Director network connections have several additional requirements:

- Do not connect VMware Cloud Director directly to the public Internet. Always protect VMware Cloud 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.

  For information on the ports that must allow incoming packets from VMware Cloud Director hosts, see VMware Ports and Protocols.

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

  For information on the ports that must allow outgoing packets from VMware Cloud Director hosts, see VMware Ports and Protocols.

- Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a denylist of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the denylist after VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Deny List.

- Route traffic between VMware Cloud Director servers and the following servers over a dedicated private network.
  - VMware Cloud Director database server
  - RabbitMQ
  - Cassandra

- If possible, route traffic between VMware Cloud 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 VMware Cloud Director transfer service is available lin VMware Knowledge Base article 2086127.

Deployment, Upgrade, and Administration of the VMware Cloud Director Appliance

3

Starting with version 9.7, the VMware Cloud Director appliance includes an embedded PostgreSQL database with a high availability function. When you deploy, upgrade, or migrate the VMware Cloud Director appliance, you can perform administration, monitoring, remediation, or troubleshooting operations.

This chapter includes the following topics:

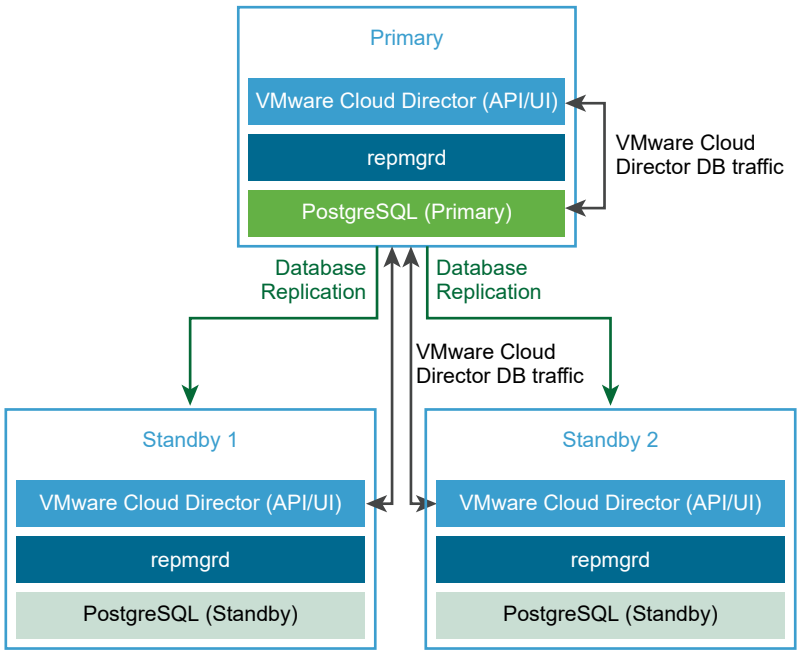
Appliance Deployments and Database High Availability Configuration

The VMware Cloud 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 VMware Cloud Director database.

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

To configure HA for your VMware Cloud 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 VMware Cloud Director appliance. You can horizontally scale your server group by additionally deploying application cells. See the Figure 3-1. VMware Cloud Director Appliance Database HA Cluster figure.

Figure 3-1. VMware Cloud Director Appliance Database HA Cluster



Creating a VMware Cloud Director Appliance Deployment with Database HA

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

1 Deploy the VMware Cloud Director appliance as a primary cell.

The primary cell is the first member in the VMware Cloud Director server group. The embedded database is configured as the VMware Cloud 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 VMware Cloud Director service health, log in with the **system administrator** credentials to the VMware Cloud Director Service Provider Admin Portal at `https://primary_eth0_ip_address/provider`.

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 VMware Cloud Director appliance as standby cells.

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

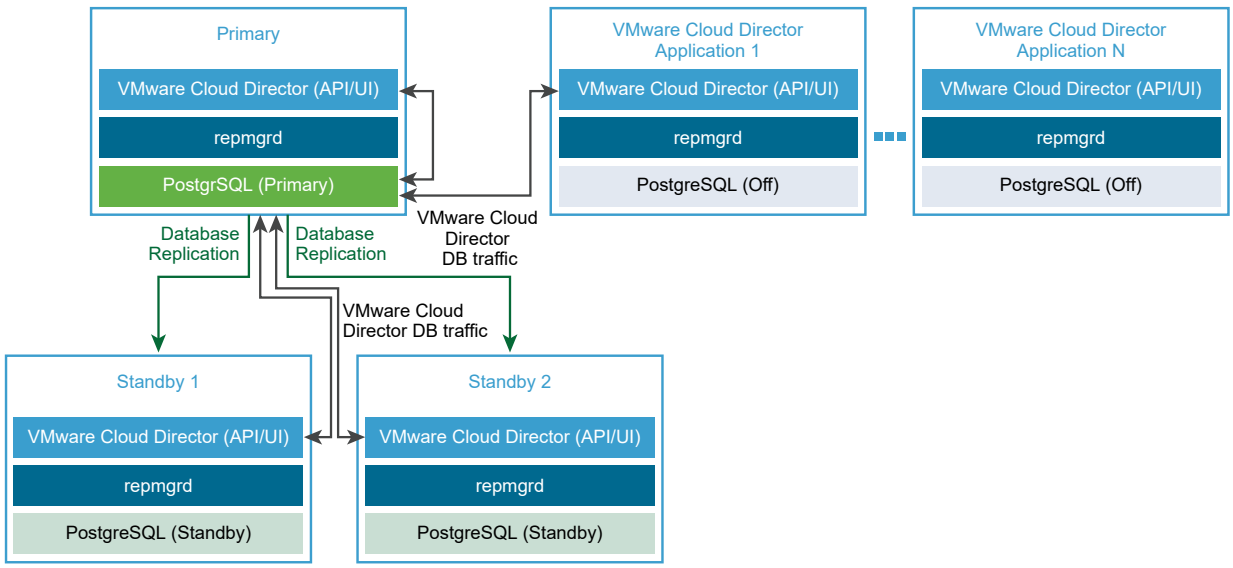
Note After the initial standby appliance deployment, the replication manager begins synchronizing its database with the primary appliance database. During this time, the VMware Cloud Director database and therefore the VMware Cloud Director UI are unavailable.

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

See View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

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

The embedded databases are not used. The VMware Cloud Director Application cell connects to the primary database.



Note If your cluster is configured for automatic failover, after you deploy one or more additional cells, you must use the Appliance API to reset the cluster failover mode to `Automatic`. See the VMware Cloud Director Appliance API. The default failover mode for new cells is `Manual`. If the failover mode is inconsistent across the nodes of the cluster, the cluster failover mode is `Indeterminate`. The `Indeterminate` mode can lead to inconsistent cluster states between the nodes and nodes following an old primary cell. To view the cluster failover mode, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

Creating a VMware Cloud Director Appliance Deployment Without Database HA

Note You can deploy a VMware Cloud 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 VMware Cloud Director server without a database HA configuration, follow this workflow:

1 Deploy the VMware Cloud Director appliance as a primary cell.

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

2 Verify that the primary cell is up and running.

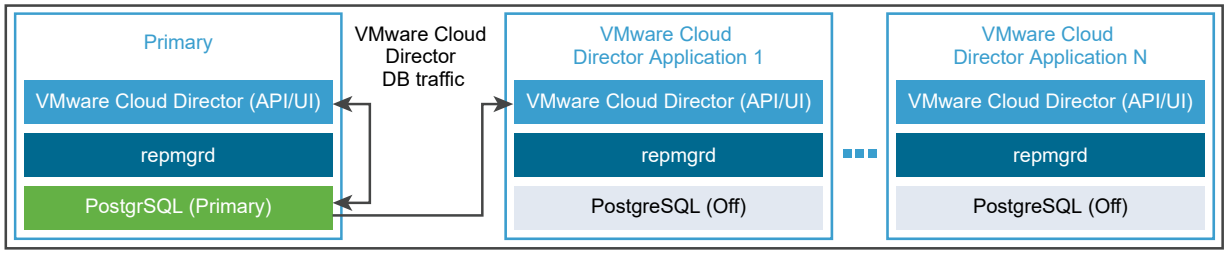
   a To verify the VMware Cloud Director service health, log in with the **system administrator** credentials to the VMware Cloud Director Service Provider Admin Portal at `https://primary_eth0_ip_address/provider`.

   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 VMware Cloud Director appliance as VMware Cloud Director Application cells.

   The embedded database is not used. The VMware Cloud Director Application cell connects to the primary database.



Automatic Failover of the VMware Cloud Director Appliance

If the primary database service fails, you can activate VMware Cloud Director to perform an automatic failover to a new primary.

The automatic failover eliminates the need for an administrator to initiate the failover action if the primary database service fails to perform its functions for any reason. By default, the failover mode is set to manual. You can set the failover mode to automatic or manual by using the VMware Cloud Director appliance API. See the *VMware Cloud Director Appliance API Schema Reference*.

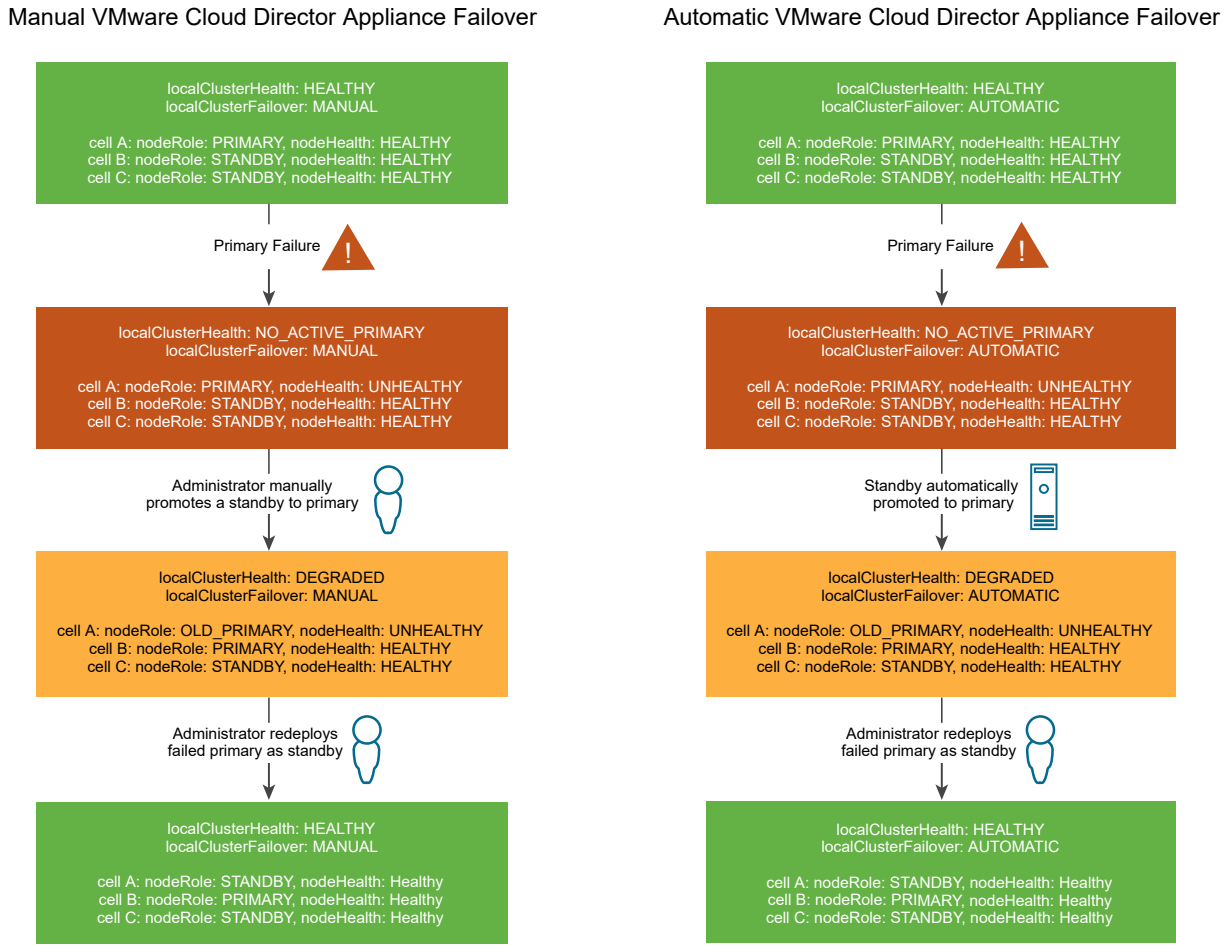
Note If your cluster is configured for automatic failover, after you deploy one or more additional cells, you must use the Appliance API to reset the cluster failover mode to `Automatic`. See the VMware Cloud Director Appliance API. The default failover mode for new cells is `Manual`. If the failover mode is inconsistent across the nodes of the cluster, the cluster failover mode is `Indeterminate`. The `Indeterminate` mode can lead to inconsistent cluster states between the nodes and nodes following an old primary cell. To view the cluster failover mode, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

If your environment has at least two active standby cells, in case of a primary database failure, a database failover is automatically initiated. After the failover, there must be at least one active standby for the new primary database to be updatable. Under normal circumstances, your VMware Cloud Director appliance deployment must have at least two active standbys at all times. If there is only one active standby for a short period, for example, due to the failure of the primary and the promotion of one of the standbys, then the old failed primary must be replaced with a new standby as soon as possible.

When there is an active primary and at least two active standby cells, the cluster is considered to be in a `Healthy` state. If there is an active primary and only one active standby, the cluster is in a `Degraded` state. If there is another database failure while the cluster is in a `Degraded` state, the primary is not updatable until another standby comes online. When the primary database is not updatable, VMware Cloud Director is not available because the VMware Cloud Director cells are unable to update the database until there is at least one active standby to process a streaming replication from the primary database. The concept of a `Healthy` and `Degraded` cluster is the same whether you activate manual or automatic failover.

After a primary database failure, the state of the primary is `No_Active_Primary`. For a manual VMware Cloud Director appliance failover, the administrator must manually promote a standby to primary and redeploy the failed primary as a standby. For automatic appliance failover, VMware Cloud Director automatically promotes a standby to primary, and the administrator manually redeploys the failed primary as a standby.

Figure 3-2. Manual and Automatic VMware Cloud Director Appliance Failover



Automatic Fencing of a Failed Primary Cell

If a new primary cell is promoted after a primary cell failure, VMware Cloud Director automatically fences out the old primary to prevent it from restarting.

In case of a failover, if a failed primary database restarts after a new primary cell is promoted, VMware Cloud Director automatically fences out the old primary. This automation prevents the split-brain syndrome where two active databases can diverge from each other. The fencing automation stops and deactivates the vpostgres service on the old primary node. After that, you can redeploy the failed primary as a standby cell to restore the cluster health to `Healthy`.

For more information about viewing the cluster health status and failover mode, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

Preparing the VMware Cloud Director Appliance Deployment

Before you deploy the VMware Cloud Director appliance, you must prepare your environment.

Preparing the Transfer Server Storage for the VMware Cloud Director Appliance

You must make an NFS or other shared storage volume accessible to all servers in a VMware Cloud Director server group. VMware Cloud Director uses the transfer server storage for appliance cluster management and for providing temporary storage for uploads, downloads, and catalog items that are published or subscribed externally.

Important The VMware Cloud Director appliance supports only NFS type of shared storage. The appliance deployment process involves mounting the NFS shared transfer server storage. The VMware Cloud Director appliance also validates most details of the NFS share during deployment, including directory permissions and ownership. You must verify that a valid NFS mount point exists and is accessible to the VMware Cloud Director appliance instances.

Each member of the server group mounts this volume at the same mountpoint: `/opt/vmware/vcloud-director/data/transfer`. Space on this volume is consumed in many ways, including:

- 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.
- VMware Cloud Director stores the appliance database backups in the `pgdb-backup` directory in the transfer share. These backup bundles might consume significant space.
- The multi-cell log bundle collector occupies this space.
- Appliance nodes data and the `response.properties` file occupy this space.

Note The volume of the transfer server storage must have the capacity for future expansion.

Note NFS downtime can cause VMware Cloud Director appliance cluster functionalities to malfunction. The appliance management UI is unresponsive while the NFS is down or cannot be reached. Other functionalities that might be affected are the fencing out of a failed primary cell, switchover, promoting a standby cell, and so on.

Note When you use Ubuntu or Debian based Linux distributions for the NFS, the creation of database backups might fail.

Shared Storage Options

A traditional Linux-based NFS server or other solutions like Microsoft Windows Server, the VMware vSAN File Service NFS feature, and so on, can provide the shared storage. Starting with vSAN 7.0, you can use the vSAN File Service functionality to export NFS shares by using NFS 3.0 and NFS 4.1 protocols. For more information about vSAN File Service, see the *Administering VMware vSAN* guide in the VMware vSphere Product Documentation.

Requirements for Configuring the NFS Server

There are specific requirements for the NFS server configuration, so that VMware Cloud 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 a multi-cell log collection.

- The export list for the NFS server must allow for each server member in your VMware Cloud 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 VMware Cloud 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.

Linux NFS Server Example

If the Linux NFS server has a directory named vCDspace as the transfer space for the VMware Cloud 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 three cells named vCD-Cell1-IP, vCD-Cell2-IP, and vCD-Cell3-IP is the `no_root_squash` method. You must add the following lines to the `/etc/exports` file.

```
/nfs/vCDspace vCD_Cell1_IP_Address(rw,sync,no_subtree_check,no_root_squash)
/nfs/vCDspace vCD_Cell2_IP_Address(rw,sync,no_subtree_check,no_root_squash)
/nfs/vCDspace vCD_Cell3_IP_Address(rw,sync,no_subtree_check,no_root_squash)
```

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.

For each server in the VMware Cloud Director server group, you must have a corresponding entry in the NFS server's `/etc/exports` file so that they can all mount this NFS share. After changing the `/etc/exports` file on the NFS server, run `exportfs -a` to re-export all NFS shares.

Install and Configure NSX Data Center for vSphere for VMware Cloud Director

If you plan your VMware Cloud 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 VMware Cloud Director installation.

NSX Manager is included in the NSX Data Center for vSphere download. For the most recent information about compatibility between VMware Cloud 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 VMware Cloud Director.

Important This procedure applies only when you are performing a new installation of VMware Cloud Director. If you are upgrading an existing installation of VMware Cloud Director, see Upgrading VMware Cloud Director on Linux.

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 VMware Cloud Director in your planned VMware Cloud Director installation.

4. Configure VXLAN support in the associated NSX Manager instances.

   VMware Cloud 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 VMware Cloud Director

If you plan your VMware Cloud Director installation to use network resources from NSX-T Data Center, you must install and configure NSX-T Data Center.

Important To configure the NSX-T Data Center objects and tools, use the simplified policy UI and the policy APIs that correspond to the simplified UI. For more information, see the overview of NSX-T Manager in the *NSX-T Data Center Administration Guide*.

For the most recent information about compatibility between VMware Cloud Director and other VMware products, see VMware Product Interoperability Matrices.

For information about the network requirements, see Network Configuration Requirements for VMware Cloud Director.

This procedure applies only when you are performing a new installation of VMware Cloud Director. If you are upgrading an existing installation of VMware Cloud Director, see Upgrading VMware Cloud Director on Linux.

Prerequisites

Familiarize yourself with NSX-T Data Center.

Procedure

1. Deploy and configure the NSX-T Manager virtual appliances.

   For more information on NSX-T Manager deployment, see the *NSX-T Data Center Installation Guide*.

2. Create transport zones based on your networking requirements.

   For more information on transport zones creation, see the *NSX-T Data Center Installation Guide*.

   Note

3. Deploy and configure Edge nodes and an Edge cluster.

   For more information on NSX Edge creation, see the *NSX-T Data Center Installation Guide*.

4. Configure the ESXi host transport nodes.

   For more information on configuring a managed host transportation node, see the *NSX-T Data Center Installation Guide*.

5. Create a tier-0 gateway.

   For more information on tier-0 creation, see the *NSX-T Data Center Administration Guide*.

What to do next

After you install VMware Cloud Director, you can:

1. Register the NSX-T Manager instance with your cloud.

For information about registering an NSX-T Manager instance, see the *VMware Cloud Director Service Provider Admin Portal Guide*.

2 Create a network pool backed by an NSX-T Data Center transport zone.

For more information on creating a network pool that is backed by an NSX-T Data Center transport zone, see the *VMware Cloud Director Service Provider Admin Portal Guide*.

3 Import the tier-0 gateway as an external network.

For more information on adding an external network that is backed by an NSX-T Data Center tier-0 logical router, see the *VMware Cloud Director Service Provider Admin Portal Guide*.

Deployment and Initial Configuration of the VMware Cloud Director Appliance

You can create a VMware Cloud Director server group by deploying one or more instances of the VMware Cloud Director appliance. You deploy the VMware Cloud Director appliance by using the vSphere Client or the VMware OVF Tool.

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

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

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-9.7.0.0-9229800_OVA10.ova`.

The VMware Cloud Director appliance package contains the following software:

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

The primary-small and standby-small VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director appliance as a primary cell, and two instances as standby cells. You can deploy additional instances of the VMware Cloud Director appliance in the server group as vCD application cells, which run only the VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Appliance Management UI Certificate.

Note The VMware Cloud Director appliance does not support external databases.

Appliance Network Configuration

Starting with version 9.7, the VMware Cloud 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.

Note The `eth0` and `eth1` networks must be placed on separate subnets.

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

After the creation of the VMware Cloud Director appliance, you can use the vSphere networking features to add a new network interface card (NIC). See the Add a Network Adapter to a Virtual Machine information in the *vSphere Virtual Machine Administration* guide.

The VMware Cloud 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.

Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify the server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after the VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Denylist.

VMware Cloud Director Appliance Sizing Guidelines

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

Overview

To ensure that the cluster can support an automated failover if a primary cell failure occurs, the minimal VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.

VMware Cloud 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 VMware Cloud Director environment	No	No	Yes
Cassandra VM metrics enablement in VMware Cloud 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 VMware Cloud Director 10.2.x `primary-large` and `standby-large` appliances, by default, do not have the 16 vCPUs required for a Large HA cluster configuration. During the deployment of the VMware Cloud Director appliance, the `primary-large` and `standby-large` appliance size options deploy an appliance with 8 vCPUs for version 10.2.2 and 4 vCPUs for version 10.2 and 10.2.1. If you want to have a Large VMware Cloud 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 VMware Cloud Director cell, the CPU or memory use grows and reaches a plateau at a high level, that is, a level near capacity. The VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director appliance to one of the supported configurations, after running the VMware Cloud 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 VMware Cloud Director appliance to a custom configuration, after running the VMware Cloud 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 1048576 (1024*1024).

```
cat /proc/meminfo | grep MemTotal | cut -dk -f1 | awk '{print int($2/1048576)}'
```

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

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

Where `floor` returns the largest integer less than or equal to the value in the square brackets.

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
```

Prerequisites for Deploying the VMware Cloud Director Appliance

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

- Verify that you have access to the VMware Cloud Director `.ova` file.
- Before you deploy the primary appliance, prepare an NFS shared transfer service storage. See Preparing the Transfer Server Storage for VMware Cloud Director on Linux.

  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.

VMware Cloud Director Appliance Deployment Methods

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

Deploy the VMware Cloud Director Appliance by Using the vSphere Client

You can deploy the VMware Cloud Director appliance as an OVF template by using the vSphere Client (HTML5). After you deploy the OVF template, you must complete the configuration in the appliance management user interface.

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

Important Mixed VMware Cloud Director installations on Linux and VMware Cloud 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 by using VMware OVF Tool. See Deploying the VMware Cloud Director Appliance by Using VMware OVF Tool.

Note Deploying the VMware Cloud Director appliance in VMware Cloud Director is unsupported.

Prerequisites

See Prerequisites for Deploying the VMware Cloud Director Appliance.

Procedure

1. Start the VMware Cloud Director Appliance Deployment

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

2. Configure the VMware Cloud Director Primary Appliance

   After you deploy the OVF Template for the primary appliance, you must continue to the configuration phase in the appliance management user interface of the primary VMware Cloud Director appliance instance.

3. Configure the VMware Cloud Director Standby and Application Cells

   After you deploy the OVF Template for a standby or application cell, you must continue to the configuration phase in the appliance management user interface of the instance you want to deploy.

What to do next

- Configure the public console proxy address, because the VMware Cloud Director appliance uses its `eth0` NIC with custom port 8443 for the console proxy service. See Customize Public Addresses for VMware Cloud Director on Linux.
- To add members to the VMware Cloud Director server group, repeat the procedure.
- To enter the license key, log in to the VMware Cloud Director Service Provider Admin Portal.
- To replace the self-signed certificate that is created during the appliance first boot, you can Create an CA-Signed SSL Certificate Keystore for VMware Cloud Director on Linux.

Start the VMware Cloud Director Appliance Deployment

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

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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director server group. The embedded database in the primary cell is configured as the VMware Cloud Director database. The database name is `vcloud`, and the database user is `vcloud`.
Primary-large	■ VMware Cloud Director 10.2.1 and later versions deploy the appliance with 24 GB of RAM and 8 vCPUs as the first member in a VMware Cloud Director server group. ■ VMware Cloud Director 10.2 deploys the appliance with 24 GB of RAM and 4 vCPUs as the first member in a VMware Cloud Director server group. The embedded database in the primary cell is configured as the VMware Cloud Director database. The database name is `vcloud`, and the database user is `vcloud`.
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 VMware Cloud 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. ■ VMware Cloud Director 10.2.1 and later versions deploy the appliance with 24 GB of RAM and 8 vCPUs as the second or the third member in a VMware Cloud Director server group with a database high availability configuration. ■ VMware Cloud Director 10.2 deploys the appliance with 24 GB of RAM and 4 vCPUs as the second or the third member in a VMware Cloud 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.
Cloud Director Cell Application	■ VMware Cloud Director 10.2.1 and later versions deploy the appliance with 8 GB of RAM and 4 vCPUs as a subsequent member in a VMware Cloud Director server group. ■ VMware Cloud Director 10.2 deploys the appliance with 8 GB of RAM and 2 vCPUs as a subsequent member in a VMware Cloud 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 VMware Cloud 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 of the wizard to configure the VMware Cloud Director details.

12 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. If you want to use FIPS mode, the **root** password for the appliance must contain 14 or more characters. **Note** The OVF deployment wizard does not validate the initial root password against password criteria.

Setting	Description
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 root login	Deactivated by default.

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

13 (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**.

If you want to reach hosts over a non-default gateway route, you might need to provide static routes. For example, management infrastructure is accessible only through the `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, 172.16.200.253`**.

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

Setting	Description
Default Gateway	The IP address of the default gateway for the appliance.
Domain Name	The DNS search domain, for example, *mydomain.com*.
Domain Search Path	A comma- or space-separated list of domain names for the appliance hostname lookup, for example, *subdomain.example.com*. **Note** The domain name that you entered in the Domain Name text box is the first element in the domain search path list.
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 Netmask	The netmask or prefix for the `eth0` interface.
eth1 Network IP Address	The IP address for the `eth1` interface.
eth1 Network Netmask	The netmask or prefix for the `eth1` interface.

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

What to do next

1 Power on the newly created virtual machine.

2 Configure the VMware Cloud Director Primary Appliance or Configure the VMware Cloud Director Standby and Application Cells.

Configure the VMware Cloud Director Primary Appliance

After you deploy the OVF Template for the primary appliance, you must continue to the configuration phase in the appliance management user interface of the primary VMware Cloud Director appliance instance.

Prerequisites

1 Start the VMware Cloud Director Appliance Deployment.

2 Power on the newly created virtual machine.

3 Familiarize yourself with the Preparing the Transfer Server Storage for the VMware Cloud Director Appliance topic.

Procedure

1 Open a Web browser and navigate to `https://Primary-Appliance-eth1-IP-Address:5480`.

2 Log in to the appliance management user interface of the primary appliance instance.

The **Primary Appliance System Setup** page appears.

3 In section **Appliance Settings**, configure the appliance details and click **Next**.

Setting	Description
NFS mount for transfer file location	The location of the NFS shared transfer server storage. VMware Cloud Director validates the location and displays a green check mark if the NFS mount is validated.
DB password for the 'vcloud' user	The password for the **vcloud** PostgreSQL database user.
Confirm DB password	Confirmation of the password for the **vcloud** PostgreSQL database user.
Participate in the Customer Experience Improvement Program	Activates or deactivates the participation in the VMware Customer Experience Improvement Program.

4 In the **Administrator Account** section, configure the system administrator details and click **Next**.

Setting	Description
User name	The user name for the **system administrator** account. Defaults to `administrator`.
Password	The password for the **system administrator** account. The password must be between 6 and 128 characters long.
Confirm Password	Confirm the password for the **system administrator** account.
Full name	The full name of the **system administrator**. Defaults to `vCD Admin`.
Email address	The email address of the **system administrator**.

5 In the **VMware Cloud Director Settings** section, configure the installation of this instance.

Setting	Description
System name	The name for the vCenter Server folder to create for this VMware Cloud Director installation.
Installation ID	The ID for this VMware Cloud Director installation to use when you create MAC addresses for virtual NICs. Defaults to `1`. If you plan to create stretched networks across VMware Cloud Director installations in multisite deployments, consider setting a unique installation ID for each VMware Cloud Director installation.

6 Click **Submit** and when the system setup finishes, click **OK**.

Results

If the deployment is successful, the **Embedded Database Availability** and **Services** tabs appear.

What to do next

- Change the VMware Cloud Director Appliance Timezone
- Deploy a standby or application cell. See Start the VMware Cloud Director Appliance Deployment.
- Configure the VMware Cloud Director Standby and Application Cells

Configure the VMware Cloud Director Standby and Application Cells

After you deploy the OVF Template for a standby or application cell, you must continue to the configuration phase in the appliance management user interface of the instance you want to deploy.

Prerequisites

1 Deploy a standby or application cell. See Start the VMware Cloud Director Appliance Deployment.

2 See Preparing the Transfer Server Storage for the VMware Cloud Director Appliance.

3 Power on the newly created virtual machine.

Procedure

1 Open a Web browser and navigate to `https://Cell-eth1-IP-Address:5480`.

2 Log in to the appliance management user interface of the standby or application cell.

The **System Setup** page appears.

3 Enter the NFS mount for the transfer file location.

4 Click **Submit** and when the system setup finishes, click **OK**.

What to do next

Change the VMware Cloud Director Appliance Timezone

Deploying the VMware Cloud Director Appliance by Using VMware OVF Tool

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

You must deploy the first member of a VMware Cloud Director server group as a primary cell. You can deploy a subsequent member of a VMware Cloud Director server group as a standby or VMware Cloud Director 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 VMware Cloud Director installations on Linux and VMware Cloud 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 VMware Cloud Director Appliance by Using the vSphere Client.

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

Starting with VMware Cloud Director 10.2, you must include the `--X:enableHiddenProperties` parameter to deploy the VMware Cloud Director appliance.

Note You can choose whether to specify the optional OVF configuration options during the primary appliance deployment, or to run the appliance management user interface to finish the configuration after the deployment.

`ovftool` Command Options and Properties for Deploying the VMware Cloud Director Appliance

Option	Value	Description
`--noSSLVerify`	n/a	Skips SSL verification for vSphere connections.
`--acceptAllEulas`	n/a	Accepts all end-user licenses agreements (EULAs).
`--X:enableHiddenProperties`	n/a	Makes visible all the properties for the configuration of the appliance.
`--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.

Option	Value	Description
--prop:"vami.searchpath.VMware_vCloud_Director"	*domain_names*	The domain search path of the appliance. A comma or space-separated list of domain names.
--prop:"vcloudconf.ceip_enabled.VMware_vCloud_Director"	true | false	Activates or deactivates the participation in the VMware Customer Experience Improvement Program. The default is true. Optional if you plan to run the appliance management user interface to finish the primary appliance configuration after the deployment.
--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"		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. Optional if you plan to run the appliance management user interface to finish the primary appliance configuration after the deployment.

Option	Value	Description
`--prop:"vcloudconf.admin_email.VMware_vCloud_Director_email"`	*email_address*	The email address of the **system administrator** account. Used only for a primary cell. Optional if you plan to run the appliance management user interface to finish the primary appliance configuration after the deployment.
`--prop:"vcloudconf.admin_fname.VMware_vCloud_Director_name"`	*Administrator*	The name for the **system administrator** account. Used only for a primary cell. Optional if you plan to run the appliance management user interface to finish the primary appliance configuration after the deployment.
`--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director_password"`	*password*	The password for the **system administrator** account. Used only for a primary cell. Optional if you plan to run the appliance management user interface to finish the primary appliance configuration after the deployment.
`--prop:"vcloudconf.admin_uname.VMware_vCloud_Director_username"`	*username*	The user name for the **system administrator** account. Used only for a primary cell. Optional if you plan to run the appliance management user interface to finish the primary appliance configuration after the deployment.
`--prop:"vcloudconf.inst_id.VMware_vCloud_Director_ID"`	*ID*	The VMware Cloud Director installation ID. Used only for a primary cell. Optional if you plan to run the appliance management user interface to finish the primary appliance configuration after the deployment.
`--prop:"vcloudconf.sys_name.VMware_vCloud_System_name"`	*name*	The name for the vCenter Server folder to create for this VMware Cloud Director installation. Optional if you plan to run the appliance management user interface to finish the primary appliance configuration after the deployment.

Option	Value	Description
`--prop:"vcloudnet.routes0.VMware_vCloud_Director_1"`	*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_Director_1"`	*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 VMware Cloud 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. ■ `primary-small` deploys the appliance with 12 GB of RAM and 2 vCPUs as the first member in a VMware Cloud Director server group. The embedded database in the primary cell is configured as the VMware Cloud Director database. The database name is `vcloud`, and the database user is `vcloud`. ■ `primary-large`: ■ VMware Cloud Director 10.2.1 and later versions deploy the appliance with 24 GB of RAM and 8 vCPUs as the first member in a VMware Cloud Director server group. ■ VMware Cloud Director 10.2 deploys the appliance with 24 GB of RAM and 4 vCPUs as the first member in a VMware Cloud Director server group. The embedded database in the primary cell is configured as the VMware Cloud 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 VMware Cloud 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`: ■ VMware Cloud Director 10.2.1 and later versions deploy the

Option	Value	Description
		appliance with 24 GB of RAM and 8 vCPUs as the second or the third member in a VMware Cloud Director server group with a database high availability configuration. ■ VMware Cloud Director 10.2 deploys the appliance with 24 GB of RAM and 4 vCPUs as the second or the third member in a VMware Cloud 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`: ■ VMware Cloud Director 10.2.1 and later versions deploy the appliance with 8 GB of RAM and 4 vCPUs as a subsequent member in a VMware Cloud Director server group. ■ VMware Cloud Director 10.2 deploys the appliance with 8 GB of RAM and 2 vCPUs as a subsequent member in a VMware Cloud 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 VMware Cloud 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 a Production Primary VMware Cloud 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 \
--X:enableHiddenProperties \
--datastore='datastore6' \
--allowAllExtraConfig  \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thick \
--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-large" \
--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 Production Standby VMware Cloud 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 \
--X:enableHiddenProperties \
--datastore='datastore6' \
```

```
--allowAllExtraConfig  \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thick \
--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-large" \
--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
```

After you deploy the VMware Cloud Director appliance

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

Use the appliance management user interface to configure the primary appliance. See Configure the VMware Cloud Director Primary Appliance.

Use the appliance management user interface to configure the standby and application cells. See Configure the VMware Cloud Director Standby and Application Cells.

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

You can deploy the VMware Cloud 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 VMware Cloud Director appliances, VMware Cloud Director generates self-signed certificates and uses them to configure the VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Appliance.

If the signed certificates you use on the primary VMware Cloud Director appliance are wildcard signed certificates, these certificates can apply to all other appliances in the VMware Cloud Director server group, that is, standby cells and VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Appliance.
- If the keystore type of the keystore containing the signed wildcard SSL certificates is JCEKS, 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.

```
/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 VMware Cloud 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.

a Run the command to stop the service.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid
cell) -s
```

b Run the command to start the service.

```
systemctl start vmware-vcd
```

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

In the VMware Cloud 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 VMware Cloud Director Appliance.

Important Upon deployment, the VMware Cloud 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_password*.

Prerequisites

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

Procedure

1. Log in directly or by using an SSH client to the VMware Cloud Director appliance console as **root**.
2. Depending on your environment needs, choose one of the following options.

   When you deploy the VMware Cloud Director appliance, VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 PKCS12 -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 PKCS12 -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 VMware Cloud Director appliance.

8 Run the commands to import the signed certificates into the PKCS12 keystore.

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

```
keytool -import -storetype PKCS12 -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 PKCS12 -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 PKCS12 -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 PKCS12 -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 PKCS12 -storepass root_password -keystore /opt/vmware/vcloud-director/
certificates.ks -list
```

10 Run the command to import the certificates into the VMware Cloud 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 VMware Cloud Director appliance.

a Run the command to stop the service.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid
cell) -s
```

b Run the command to start the service.

```
systemctl start vmware-vcd
```

What to do next

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

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

If you have your own private key and CA-signed certificate files, before importing the keystores to your VMware Cloud 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 VMware Cloud Director appliance. VMware Cloud 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 by using an SSH client to the VMware Cloud 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 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.p12 -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.p12 -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 `certificates.ks` keystore.

   a Import the PKCS12 keystore for the HTTPS service.

   ```
   keytool -importkeystore -deststorepass keystore_password -destkeystore /opt/vmware/
   vcloud-director/certificates.ks -deststoretype PKCS12 -srckeystore http.p12
   -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 PKCS12 -srckeystore consoleproxy.p12
   -srcstoretype PKCS12 -srcstorepass keystore_password
   ```

6 Verify that the import of the certificates is successful.

   ```
   keytool -storetype PKCS12 -storepass keystore_password -keystore /opt/vmware/vcloud-
   director/certificates.ks -list
   ```

7 Run the command to import the signed certificates into the VMware Cloud 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 VMware Cloud Director appliance.

   ```
   service vmware-vcd restart
   ```

What to do next

- If you are using wildcard certificates, see Deploy the VMware Cloud Director Appliance with Signed Wildcard Certificates for HTTPS and Console Proxy Communication.

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

After You Deploy the VMware Cloud Director Appliance

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

After the creation of the VMware Cloud Director appliance, you can use the vSphere networking features to add a new network interface card (NIC). See the Add a Network Adapter to a Virtual Machine information in the *vSphere Virtual Machine Administration* guide.

Note If your cluster is configured for automatic failover, after you deploy one or more additional cells, you must use the Appliance API to reset the cluster failover mode to `Automatic`. See the VMware Cloud Director Appliance API. The default failover mode for new cells is `Manual`. If the failover mode is inconsistent across the nodes of the cluster, the cluster failover mode is `Indeterminate`. The `Indeterminate` mode can lead to inconsistent cluster states between the nodes and nodes following an old primary cell. To view the cluster failover mode, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify the server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after the VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Denylist.

Change the VMware Cloud Director Appliance Timezone

After you deploy successfully the VMware Cloud Director appliance, you can change the system time zone of the appliance. All VMware Cloud Director appliance instances in the server group and the transfer server storage must use the same settings.

Prerequisites

- Deploy the VMware Cloud Director appliance. See Deployment and Initial Configuration of the VMware Cloud Director Appliance.
- Change the transfer server storage timezone to the new timezone of the VMware Cloud Director primary appliance.

Procedure

1. By using a Web Console or a Remote Console for the primary node, on the bottom left of the console window, select **Set Timezone**.
2. Select a location, a country, and a time zone region.

   The newly selected time zone appears on the bottom left of the console window.
3. Log in to the VMware Cloud Director appliance console as **root**.
4. To ensure that the VMware Cloud Director appliance uses the new time zone, restart the `vmware-vcd` service.
5. Repeat Step 1 to Step 4 for any standby and application cells in your VMware Cloud Director deployment.

Customize Public Addresses for the VMware Cloud Director Appliance

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

You must configure the VMware Cloud Director public console proxy address, because the appliance uses a single IP address with custom port 8443 for the console proxy service. See 6.

Prerequisites

Verify that you are logged in as a **system administrator**. Only a **system administrator** can customize the public endpoints.

Procedure

1. From the top navigation bar of the Service Provider Admin Portal, select **Administration**.
2. In the left panel, under **Settings**, click **Public Addresses**.
3. To customize the public endpoints, click **Edit**.
4. To customize the VMware Cloud Director URLs, edit the **Web Portal** endpoints.
   a. Enter a custom VMware Cloud Director public URL for HTTPS (secure) connections and click **Upload** to upload the certificates that establish the trust chain for that endpoint.

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

5 (Optional) To customize the Cloud Director REST API and OpenAPI URLs, turn off the **Use Web Portal Settings** toggle.

   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 VMware Cloud Director API at `http://vcloud.example.com/api`, and you can access the VMware Cloud Director OpenAPI at `http://vcloud.example.com/cloudapi`.

   b Enter a custom HTTPS REST API base URL and click **Upload** 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 VMware Cloud Director API at `https://vcloud.example.com/api`, and you can access the VMware Cloud Director 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 VMware Cloud 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 the `PEM` format without a private key.

6 Enter a custom VMware Cloud Director public console proxy address.

   This address is the fully qualified domain name (FQDN) of the VMware Cloud Director appliance `eth0` NIC, specified either by FQDN or IP address, with custom port 8443 for the console proxy service.

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

   VMware Cloud Director uses the console proxy address when opening a remote console window on a VM.

7 To save your changes, click **Save**.

Install and Configure a Cassandra Database for Storing Historic Metric Data

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. Retrieval of current metrics does not require optional database software.

Prerequisites

- Verify that VMware Cloud 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 *VMware Cloud 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 VMware Cloud 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 Chapter 5 Cell Management Tool Reference.

2 (Optional) If you are upgrading VMware Cloud 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 VMware Cloud Director cell.

Install and Configure a RabbitMQ AMQP Broker

If you want to use blocking tasks, notifications, or VMware Cloud Director API extensions, like Container Service Extension (CSE) and VMware Cloud Director App Launchpad, you must install and configure a RabbitMQ AMQP Broker.

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

For VMware Cloud Director, using an MQTT client can be an alternative to the RabbitMQ AMQP Broker when configuring notifications. See Subscribe to Events, Tasks, and Metrics by Using an MQTT Client.

Procedure

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

   See the *VMware Cloud 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 VMware Cloud Director cell.

3 During the RabbitMQ installation, make a note of the values that are required for configuring VMware Cloud 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` for non-SSL. The default port for SSL/TLS is `5671`.
   - The communication protocol is TCP.
   - The RabbitMQ virtual host. The default is "`/`".

What to do next

By default, the VMware Cloud 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 VMware Cloud Director cell, typically at `$VCLOUD_HOME/jre/lib/security/cacerts`.

To enable SSL with the VMware Cloud Director AMQP service, see the Configure an AMQP Broker information in the *VMware Cloud Director Service Provider Admin Portal Guide*.

Change the VMware Cloud Director Appliance Root Password

When you change the root password for a VMware Cloud Director appliance, you must also update the appliance certificate keystore to use the new password.

Prerequisites

- Familiarize yourself with the `keytool` command. VMware Cloud Director places a copy of keytool at `/opt/vmware/vcloud-director/jre/bin/keytool`.
- If you are using wildcard certificates and you are storing them on the NFS shared transfer storage, to ensure that they are updated, follow the procedure described in Deploy the VMware Cloud Director Appliance with Signed Wildcard Certificates for HTTPS and Console Proxy Communication.

Procedure

1. Log in directly or by using an SSH client to the VMware Cloud Director appliance console as **root**.
2. Run the `passwd` command and change the password for the **root** user.

   ```
   passwd root
   ```

   Note If FIPS mode is enabled, the **root** password of the appliance must contain at least 14 characters.

   Note If the root password is already expired, VMware Cloud Director prompts you to set it the first time when you log in to the VMware Cloud Director appliance console as **root**.
3. Run the command to back up the existing certificates keystore file.

   ```
   cp /opt/vmware/vcloud-director/certificates.ks /tmp/certificates.ks
   ```

4 To generate a new certificates keystore, run the `keytool` command.

```
keytool -importkeystore -srckeystore /opt/vmware/vcloud-director/certificates.ks
-srcstoretype PKCS12 -srcstorepass old_root_password -destkeystore /opt/vmware/vcloud-
director/certificates-new.ks -deststoretype PKCS12 -deststorepass new_root_password
-destkeypass new_root_password
```

Note Starting with VMware Cloud Director 10.2, the default certificate keystore type for the VMware Cloud Director appliance is PKCS12. If you are using a version of the appliance that was upgraded to version 10.2, use JCEKS as the `-srcstoretype` and `-deststoretype`.

```
keytool -importkeystore -srckeystore /opt/vmware/vcloud-director/certificates.ks
-srcstoretype JCEKS -srcstorepass old_root_password -destkeystore /opt/vmware/vcloud-
director/certificates-new.ks -deststoretype JCEKS -deststorepass new_root_password
-destkeypass new_root_password
```

5 Run the command to replace the old certificates keystore file with the new one.

```
mv /opt/vmware/vcloud-director/certificates-new.ks /opt/vmware/vcloud-director/
certificates.ks
```

6 To verify the user and group ownership of the keystore file, run the `chown` command.

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

7 To use the keystore's new password, update the VMware Cloud Director server configuration:

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

What to do next

Repeat this procedure on each appliance in the cluster.

Important All appliances must share the same root password. Any newly deployed appliance must use the new root password.

Upgrading and Migrating the VMware Cloud Director Appliance

Starting with version 9.7, the VMware Cloud Director appliance includes an embedded PostgreSQL database with a high availability function. You can upgrade the VMware Cloud Director appliance to a later version. You can also migrate your existing earlier version of VMware Cloud Director with an external PostgreSQL database to a VMware Cloud Director environment that consists of VMware Cloud Director appliance deployments version 10.0 or later.

Upgrading the VMware Cloud Director Appliance

For the upgrade of VMware Cloud Director appliance version 9.7 to version 10.2, see Upgrade the VMware Cloud Director Appliance by Using an Update Package.

Starting with VMware Cloud Director 10.0, Microsoft SQL Server databases are unsupported.

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

- The database software you are currently using for the VMware Cloud Director database. For more information, see the Upgrade and Migration Paths table.
- The VMware vSphere ® release you are currently using.
- The VMware NSX® release that you are currently using.
- Any third-party components that directly interact with VMware Cloud Director.

For information about the compatibility of VMware Cloud 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 your vSphere or NSX components as part of the VMware Cloud Director upgrade, you must upgrade them after the upgrade of VMware Cloud Director. See After You Upgrade VMware Cloud Director.

After you upgrade at least one VMware Cloud Director server, you can upgrade the VMware Cloud Director database. The database stores information about the runtime state of the server, including the state of all VMware Cloud 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 VMware Cloud Director database:

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

The upgrade requires sufficient VMware Cloud 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.`

Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify the server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after the VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Denylist.

Important After upgrading to version 10.1 and later, VMware Cloud Director always verifies certificates for any infrastructure endpoints connected to it. This is due to a change in the way VMware Cloud Director manages SSL certificates. If you do not import your certificates into VMware Cloud Director before the upgrade, the vCenter Server and NSX connections might show failed connection errors due to SSL verification issues. In this case, after upgrading, you have two options:

1. Run the cell management tool `trust-infra-certs` command to import automatically all certificates into the centralized certificate store. See Import Endpoints Certificates from vSphere Resources.
2. In the Service Provider Admin Portal UI, select each vCenter Server and NSX instance, and reenter the credentials while accepting the certificate.

Migrating the VMware Cloud Director Appliance

If your existing VMware Cloud Director server group consists of VMware Cloud Director 9.5 appliance deployments, you can only migrate your environment to a more recent version of the VMware Cloud Director appliance. Use the VMware Cloud Director installer for Linux to upgrade the existing environment only as part of the migration workflow. See Migrating to vCloud Director Appliance.

If your VMware Cloud Director environment uses an external Oracle database or an external Microsoft SQL database, you must migrate to a PostgreSQL database before upgrading to VMware Cloud Director 10.2. For upgrade paths, see Upgrading VMware Cloud Director on Linux.

Upgrade and Migration Paths and Workflows

Source environment	Target environment VMware Cloud Director appliance 10.2 with an embedded PostgreSQL database
VMware Cloud Director 9.7 on Linux with an external Microsoft SQL Server database	1 Migrate to VMware Cloud Director appliance 9.7. See Migrating vCloud Director with an External Microsoft SQL Database to vCloud Director Appliance. 2 Upgrade your environment to VMware Cloud Director appliance 10.2. See Upgrade the VMware Cloud Director Appliance by Using an Update Package.
VMware Cloud Director 9.7 on Linux with an external PostgreSQL database	1 Migrate to VMware Cloud Director appliance 9.7. See Migrating vCloud Director with an External PostgreSQL Database to vCloud Director Appliance. 2 Upgrade your environment to VMware Cloud Director appliance 10.2. See Upgrade the VMware Cloud Director Appliance by Using an Update Package.
VMware Cloud Director 10.0 on Linux with an external PostgreSQL database	1 Migrate to VMware Cloud Director appliance 10.0. See Migrating vCloud Director with an External PostgreSQL Database to vCloud Director Appliance. 2 Upgrade your environment to VMware Cloud Director appliance 10.2. See Upgrade the VMware Cloud Director Appliance by Using an Update Package.
VMware Cloud Director 10.1 on Linux with an external PostgreSQL database	1 Migrate to VMware Cloud Director appliance 10.1. See Migrating VMware Cloud Director with an External PostgreSQL Database to VMware Cloud Director Appliance. 2 Upgrade your environment to VMware Cloud Director appliance 10.2. See Upgrade the VMware Cloud Director Appliance by Using an Update Package.
VMware Cloud Director appliance 9.7, 10.0, or 10.1 with an embedded PostgreSQL database	Upgrade your environment to VMware Cloud Director appliance 10.2. See Upgrade the VMware Cloud Director Appliance by Using an Update Package.

Upgrade the VMware Cloud Director Appliance by Using an Update Package

You can upgrade the VMware Cloud Director appliance to the latest version or apply patches to the VMware Cloud Director appliance by using an update package.

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

After you apply the upgrade to every VMware Cloud Director appliance and the database upgrade is complete, you must reboot each VMware Cloud Director appliance.

Prerequisites

Take a snapshot of the primary VMware Cloud Director appliance.

1. When upgrading from version 10.1 or later or when patching, if the automatic failover in case of a primary database service failure is enabled, change the failover mode to `Manual` during the upgrade. After the upgrade, you can set the failover mode to `Automatic`. See Automatic Failover of the VMware Cloud Director Appliance.
2. Log in to the vCenter Server instance on which resides the primary VMware Cloud Director appliance of your database high availability cluster.
3. Navigate to the primary VMware Cloud Director appliance, right-click it, and click **Power > Shut Down Guest OS**.
4. Right-click the appliance and click **Snapshots > Take Snapshot**. Enter a name and, optionally, a description for the snapshot, and click **OK**.
5. Right-click the VMware Cloud Director appliance and click **Power > Power On**.
6. Verify that all nodes in your database high availability configuration are in a good state. See View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

Procedure

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

   Make a note of the primary appliance name. You must upgrade the primary appliance before the standby and application cells. You must use the primary appliance when backing up the database.

2. Download the update package to the appliance you are upgrading.

   Note You must upgrade the primary appliance first.

   VMware Cloud Director is distributed as an executable file with a name of the form `VMware_Cloud_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_Cloud_Director_10.1.0.4424-14420378_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_Cloud_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 upgrade release appears as an `Available Update`.

7 Shut down VMware Cloud Director by running the following command:

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

8 Apply the available upgrade.

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

9 Repeat 2 to 8 on the remaining standby and application cells.

10 From the primary appliance, back up the VMware Cloud Director appliance embedded database.

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

11 From any appliance, run the VMware Cloud Director database `upgrade` utility.

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

12 Reboot each VMware Cloud Director appliance.

```
shutdown -r now
```

What to do next

- If the upgrade is successful, you can delete the snapshot of the VMware Cloud Director appliance.
- If the upgrade is not successful, you can roll back the VMware Cloud Director appliance to the snapshot that you took before the upgrade. See Roll Back a VMware Cloud Director Appliance When an Upgrade Fails.

Upgrade the VMware Cloud Director Appliance by Using the VMware Update Repository

You can use the VMware Update Repository to upgrade the VMware Cloud Director appliance from version 9.7 to version 10.0 and later or apply patches.

Note You can use the VMware Update Repository only to upgrade VMware Cloud Director to the most recent VMware Cloud Director version. Only the most recent version is available in the VMware Update Repository. If you want to upgrade VMware Cloud Director to a different version, see Upgrade the VMware Cloud Director Appliance by Using an Update Package.

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

After you apply the upgrade to every VMware Cloud Director appliance and the database upgrade is complete, you must reboot each VMware Cloud Director appliance.

Prerequisites

- Take a snapshot of the primary VMware Cloud Director appliance.
  a. When upgrading from version 10.1 or later or when patching, if the automatic failover in case of a primary database service failure is enabled, change the failover mode to `Manual` for the duration of the upgrade. After the upgrade, you can set the failover mode to `Automatic`. See Automatic Failover of the VMware Cloud Director Appliance.
  b. Log in to the vCenter Server instance on which resides the primary VMware Cloud Director appliance of your database high availability cluster.
  c. Navigate to the primary VMware Cloud Director appliance, right-click it, and click **Power > Shut Down Guest OS**.
  d. Right-click the appliance and click **Snapshots > Take Snapshot**. Enter a name and, optionally, a description for the snapshot, and click **OK**.
  e. Right-click the VMware Cloud Director appliance and click **Power > Power On**.
  f. Verify that all nodes in your database high availability configuration are in a good state. See View the VMware Cloud Director Appliance Cluster Health and Failover Mode.
- Verify that the VMware Cloud Director appliance has access to `https://vapp-updates.vmware.com`.

Procedure

1 In a Web browser, log in to the appliance management user interface of a VMware Cloud 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 when backing up the database.

2 Log in directly or by using an SSH client to the primary appliance console as **root**.

3 Reset the update repository to point to the VMware Update Repository.

```
vamicli update --repo ""
```

4 Check for updates to verify that the VMware Update Repository has the desired upgrade.

   By default the `vamicli` command points to the VMware Update Repository.

```
vamicli update --check
```

   The upgrade release appears as an `Available Update`.

5 Shut down VMware Cloud Director by running the following command:

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

6 Continuing from the primary appliance, back up the VMware Cloud Director appliance embedded database.

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

   Note You must backup the appliance only once. Do not back up the appliance after applying the available upgrade.

7 Apply the available upgrade.

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

8 Log in to the remaining standby and application cells and repeat steps 3, 4, 5, and 7 on each appliance.

9 From any appliance, run the VMware Cloud Director database `upgrade` utility.

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

10 Reboot each VMware Cloud Director appliance.

```
shutdown -r now
```

What to do next

- If the upgrade is successful, you can delete the snapshot of the VMware Cloud Director appliance.
- If the upgrade is not successful, you can roll back the VMware Cloud Director appliance to the snapshot that you took before the upgrade. See Roll Back a VMware Cloud Director Appliance When an Upgrade Fails.
- If there is a `vamicli update --install latest` command failure, see Installing the Latest Update of VMware Cloud Director Fails.

Roll Back a VMware Cloud Director Appliance When an Upgrade Fails

If the upgrade of a VMware Cloud Director appliance fails, you can use the snapshot of the appliance that you took before the upgrade and roll back the VMware Cloud Director appliance.

Before you begin the rollback, use the VMware Cloud Director appliance API to make a note of the node IDs of the standby nodes in the cluster. See the *VMware Cloud Director Appliance API Schema Reference* on http://code.vmware.com.

1 Revert the primary VMware Cloud Director appliance to the snapshot that you took before you started the upgrade.

  Read how to restore virtual machine snapshots by using the revert options. See Restore VM Snapshots Using Revert in the *vSphere Virtual Machine Administration Guide*.

2 Power on the primary VMware Cloud Director appliance cell.

3 Log in directly or by using an SSH client to the OS of each VMware Cloud Director appliance cell. You must log in as a **root** user.

4 Stop the VMware Cloud Director services on all appliance cells.

```
service vmware-vcd stop
```

5 Use the primary VMware Cloud Director cell to unregister the secondary nodes in the cluster.

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

  b Change the user to **postgres**.

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

  c Run the command to unregister a standby appliance cell.

  To unregister a standby node that is not running, you must provide the node ID.

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

  d Repeat 5.c to unregister the other standby appliance cell.

6 In the vSphere Client, shut down and delete all standby appliances.

   a In the vSphere Client, navigate to the standby appliances.

   b Right-click a standby appliance and click **Power > Shut Down Guest OS**.

   c Right-click the appliance and click **Delete From Disk**.

   d Repeat 6.a through 6.c for the other standby appliance cell.

7 Verify that the `repmgr` tool suite and the embedded PostgreSQL database of the primary VMware Cloud Director appliance cell are working properly.

   a Change the user to **postgres**.

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

   b Run the command to check the cluster status.

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

   The console output shows information about the only node in the cluster.

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

8 Redeploy the secondary appliances. See Deploy the VMware Cloud Director Appliance by Using the vSphere Client.

9 Log in directly or by using an SSH client to the OS of each VMware Cloud Director appliance cell. You must log in as a **root** user.

10 Start the VMware Cloud Director services.

   ```
   service vmware-vcd start
   ```

Migrating VMware Cloud Director with an External PostgreSQL Database to VMware Cloud Director Appliance

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

The migration workflow includes four major stages.

- Upgrading the existing VMware Cloud Director environment
- Creating the new VMware Cloud Director server group by deploying one or more instances of the VMware Cloud Director 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 or later.

2 Upgrade your current VMware Cloud Director environment to version 10.2.

See Upgrading VMware Cloud Director on Linux.

3 Verify that the migration source VMware Cloud Director restart is successful.

4 On each cell of the upgraded VMware Cloud Director environment, run the command to stop the VMware Cloud 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 VMware Cloud 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`, `proxycertificates`, and `truststore` 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 VMware Cloud 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 VMware Cloud Director 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 Deployment and Initial Configuration of the VMware Cloud Director Appliance.

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

a Back up the properties, truststore, and 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 7 a.

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

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 VMware Cloud 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 VMware Cloud Director Service Fails When Migrating or Restoring to VMware Cloud Director Appliance.

d Run the command to start the VMware Cloud Director service.

```
service vmware-vcd start
```

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

15 Modify your load balancer configuration to include all new appliance `eth0` IPs in the load balancer pools for HTTP, HTTPS, and TCP traffic, and remove the old Linux VMware Cloud Director cell IPs from those pools.

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

a Open the Service Provider Admin Portal by using the `eth0` network IP address of any cell from the new server group, `https://`*`eth0_IP_new_cell`*`/provider`.

b Log in to the Service Provider Admin Portal with your existing **system administrator** credentials from the migration source.

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

17 After the successful verification of the VMware Cloud Director migration, use the Service Provider Admin Portal to delete the disconnected cells that belong to the old VMware Cloud Director environment.

a From the top navigation bar, under **Resources**, select **Cloud Resources**.

b In the left panel, click **Cloud Cells**.

c Select an inactive cell and click **Unregister**.

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

What to do next

The new migrated VMware Cloud 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 VMware Cloud 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 VMware Cloud Director

After you upgrade all VMware Cloud 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 VMware Cloud Director installation.

Important VMware Cloud 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.

Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify the server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after the VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Denylist.

Important After upgrading to version 10.1 and later, VMware Cloud Director always verifies certificates for any infrastructure endpoints connected to it. This is due to a change in the way VMware Cloud Director manages SSL certificates. If you do not import your certificates into VMware Cloud Director before the upgrade, the vCenter Server and NSX connections might show failed connection errors due to SSL verification issues. In this case, after upgrading, you have two options:

1 Run the cell management tool `trust-infra-certs` command to import automatically all certificates into the centralized certificate store. See Import Endpoints Certificates from vSphere Resources.

2 In the Service Provider Admin Portal UI, select each vCenter Server and NSX instance, and reenter the credentials while accepting the certificate.

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

Before you upgrade a vCenter Server and ESXi hosts registered to VMware Cloud 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 VMware Cloud Director, whether or not any VMware Cloud 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 VMware Cloud 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 VMware Cloud Director and NSX Manager, you must upgrade the vCenter Server systems and ESXi hosts that are registered to VMware Cloud 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. From the top navigation bar of the VMware Cloud Director Service Provider Admin Portal, under **Resources**, select **vSphere Resources**.
   b. In the left panel, click **vCenter Server Instances**.
   c. Select the radio button next to the vCenter Server instance you want to deactivate and click **Disable**.
   d. Click **OK**.
2. Upgrade the vCenter Server system.

   For information, see *vCenter Server Upgrade*.

3 Verify all VMware Cloud Director public URLs and certificate chains.

   a From the top navigation bar, select **Administration**.

   b In the left panel, under **Settings**, click **Public Addresses**.

   c Verify all public addresses.

4 Refresh the vCenter Server registration with VMware Cloud Director.

   a From the top navigation bar of the VMware Cloud Director Service Provider Admin Portal, under **Resources**, select **vSphere Resources**.

   b In the left panel, click **vCenter Server Instances**.

   c Select the radio button next to the target vCenter Server and click **Reconnect**.

   d Click **OK**.

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 VMware Cloud 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 VMware Cloud Director to upgrade an NSX Edge Gateway, you must operate on the VMware Cloud Director network object that the Edge supports:
     - An appropriate upgrade of an Edge Gateway occurs automatically when you use either the VMware Cloud Director or VMware Cloud Director API to reset a network that the Edge Gateway serves.

- Redeploying an Edge Gateway upgrades the associated NSX Edge appliance.

  Note Redeploying is supported only for NSX Data Center for vSphere Edge Gateways.

- Resetting a vApp network from within the context of the vApp upgrades the NSX Edge appliance associated with that network. To reset a vApp network from within the context of a vApp, navigate to the **Networks** tab for the vApp, display its networking details, click the radio button next to the name of the vApp network, and click **Reset**.

For more information on how to redeploy Edge Gateways and reset vApp networks, see the *VMware Cloud Director API Programming Guide*.

What to do next

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

VMware Cloud Director Appliance Administration

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 VMware Cloud Director appliance, you cannot change the `eth0` and `eth1` network IP addresses or the hostname of the appliance. If you want the VMware Cloud 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.

Note If your cluster is configured for automatic failover, after you deploy one or more additional cells, you must use the Appliance API to reset the cluster failover mode to `Automatic`. See the VMware Cloud Director Appliance API. The default failover mode for new cells is `Manual`. If the failover mode is inconsistent across the nodes of the cluster, the cluster failover mode is `Indeterminate`. The `Indeterminate` mode can lead to inconsistent cluster states between the nodes and nodes following an old primary cell. To view the cluster failover mode, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

Embedded Database Backup and Restore of VMware Cloud Director Appliance

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

Back up the VMware Cloud Director Appliance Embedded Database

If your environment consists VMware Cloud Director appliance deployments with embedded PostgreSQL databases, you can back up the VMware Cloud 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 by using an SSH client to the primary cell as **root**.
2. Back up the VMware Cloud Director appliance embedded database by running the following command.

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

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`, `proxycertificates`, and `truststore` files of the primary cell.

Restore a VMware Cloud Director Appliance 10.2.1 and Earlier Environment with a High Availability Database Configuration

If you backed up the embedded PostgreSQL database of a VMware Cloud Director appliance 10.2.1 and earlier environment with an HA database configuration, you can deploy a new appliance cluster and restore the appliance database in it.

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 VMware Cloud Director Appliance Embedded Database.
- Deploy one primary database cell and two standby database cells. See Deployment and Initial Configuration of the VMware Cloud 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 VMware Cloud 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 VMware Cloud Director version 9.7.0.1 to version 10.2.1.

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 VMware Cloud 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 VMware Cloud Director version 9.7.0.1 to version 10.2.1.

```
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 VMware Cloud Director version 9.7.0.1 to version 10.2.1.

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 following commands to reconfigure the VMware Cloud 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 --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
```

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
ssl true
```

Where:

- The `--keystore-password` option matches the keystore password for the certificates on the appliance. The keystore password might be the **root** password you used during the appliance deployment.
- The `--database-password` option matches the database password that you set during the appliance setup in the VMware Cloud Director appliance management UI at `https://appliance_eth0_ip:5480`.
- 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 VMware Cloud Director Service Fails When Migrating or Restoring to VMware Cloud Director Appliance.

e Run the command to start the VMware Cloud 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 Deployment and Initial Configuration of the VMware Cloud Director Appliance.

7 If the new appliances use different IPs than the original appliances that you are replacing, you must update the configuration of the load balancer which fronts the VMware Cloud Director server group to include the IPs of the new appliances.

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

a Open the VMware Cloud Director Service Provider Admin Portal by using the `eth0` network IP address of any cell from the new server group, `https://et0_IP_new_cell/provider`.

If you updated the load balancer configuration as per step 7, you must use the public address of the server group to access the Service Provider Admin Portal.

b Log in to the Service Provider Admin Portal with your existing **system administrator** credentials.

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

9 After the successful verification of the database restore, use the Service Provider Admin Portal to delete the disconnected cells that belong to the old VMware Cloud Director environment.

a From the top navigation bar, under **Resources**, select **Cloud Resources**.

b In the left panel, click **Cloud Cells**.

c Select an inactive cell and click **Unregister**.

10 If the failover mode before the restore was `Automatic`, you must set it again to `Automatic` by using the VMware Cloud Director appliance API.

Restore a VMware Cloud Director Appliance 10.2.2 and Later Environment with a High Availability Database Configuration

If you backed up the embedded PostgreSQL database of a VMware Cloud Director appliance 10.2.2 and later environment with an HA database configuration, you can deploy a new appliance cluster and restore the appliance database in it.

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 VMware Cloud Director Appliance Embedded Database.
- Deploy one primary database cell and two standby database cells. See Deployment and Initial Configuration of the VMware Cloud 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 VMware Cloud 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.pem`, `certificates.key`, `proxycertficates.pem`, `proxycertficates.key`, `truststore.pem`, and the database dump file named `vcloud_date_time_format`.

Note The `truststore.pem` file is only available for VMware Cloud Director 10.2.2 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 VMware Cloud Director service.

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

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

Note The `truststore.pem` file is only available for VMware Cloud Director 10.2.2 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.pem` file is only available for VMware Cloud Director 10.2.2 and later.

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 following commands to reconfigure the VMware Cloud 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 --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
```

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-
ssl true
```

Where:

- The `--keystore-password` option matches the keystore password for the certificates on the appliance. The keystore password might be the **root** password you used during the appliance deployment.

- The `--database-password` option matches the database password that you set during the appliance setup in the VMware Cloud Director appliance management UI at `https://appliance_eth0_ip:5480`.
- 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 VMware Cloud Director Service Fails When Migrating or Restoring to VMware Cloud Director Appliance.

e Run the command to start the VMware Cloud 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 Deployment and Initial Configuration of the VMware Cloud Director Appliance.

7 If the new appliances use different IPs than the original appliances that you are replacing, you must update the configuration of the load balancer which fronts the VMware Cloud Director server group to include the IPs of the new appliances.

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

a Open the VMware Cloud Director Service Provider Admin Portal by using the `eth0` network IP address of any cell from the new server group, `https://et0_IP_new_cell/provider`.

If you updated the load balancer configuration as per step 7, you must use the public address of the server group to access the Service Provider Admin Portal.

b Log in to the Service Provider Admin Portal with your existing **system administrator** credentials.

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

9 After the successful verification of the database restore, use the Service Provider Admin Portal to delete the disconnected cells that belong to the old VMware Cloud Director environment.

a From the top navigation bar, under **Resources**, select **Cloud Resources**.

b In the left panel, click **Cloud Cells**.

c Select an inactive cell and click **Unregister**.

10 If the failover mode before the restore was `Automatic`, you must set it again to `Automatic` by using the VMware Cloud Director appliance API.

11 If the VMware Cloud Director appliance FIPS mode was on before the restore, you must set it again by using the VMware Cloud Director appliance API.

   The cell FIPS mode restores automatically.

Changing the Failover Mode of the VMware Cloud Director Appliance

By default, the VMware Cloud Director appliance is in manual failover mode and if the primary database service fails, you must initiate the failover action. You can change the failover mode to automatic by using the appliance API.

Starting with VMware Cloud Director 10.1, if the primary database service fails, you can enable VMware Cloud Director to perform an automatic failover to a new primary. See Automatic Failover of the VMware Cloud Director Appliance.

The failover mode is set to `automatic` or `manual` by using the VMware Cloud Director appliance API. See the *Failovermode* section of the VMware Cloud Director Appliance API Schema Reference.

For clusters configured with automatic failover, after you deploy one or more additional cells, you must use the appliance API to reset the failover mode of the cluster to `automatic`. If you do not reset the failover mode of the cluster, the failover mode across the nodes becomes inconsistent.

Configure External Access to the VMware Cloud Director Database

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

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

Procedure

1 Log in directly or by using an SSH client 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 VMware Cloud 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.

Prerequisites

To make the changes to the OVF properties permanent, you must use the vSphere UI to change the OVF property values. See the Configure vApp Properties topic in the *vSphere Virtual Machine Administration* guide.

Procedure

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

   a Log in directly or by using an SSH client to the VMware Cloud 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`**.

Activate or Deactivate FIPS Mode on the VMware Cloud Director Appliance

Starting with version 10.2.2, you can configure the VMware Cloud Director appliance to use FIPS 140-2 validated cryptographic modules and to run in FIPS-compliant mode.

The Federal Information Processing Standard (FIPS) 140-2 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. The NIST Cryptographic Module Validation Program (CMVP) validates the cryptographic modules compliant with the FIPS 140-2 standards.

The goal of VMware Cloud Director FIPS support is to ease the compliance and security activities in various regulated environments. To learn more about support for FIPS 140-2 in VMware products, see https://www.vmware.com/security/certifications/fips.html.

VMware Cloud Director FIPS-validated cryptography is deactivated by default. By activating FIPS mode, you configure VMware Cloud Director to use FIPS 140-2 validated cryptographic modules and to run in FIPS-compliant mode.

Note Activating FIPS mode also activates reverse lookup of host names.

Important When you activate FIPS mode, the integration with vRealize Orchestrator does not work.

In VMware Cloud Director 10.2.2 when you activate FIPS mode, you cannot encrypt SAML assertions. When not in FIPS mode, there is no restriction on assertion encryption.

VMware Cloud Director uses the following FIPS 140-2 validated cryptographic modules:

- VMware's BC-FJA (Bouncy Castle FIPS Java API), version 1.0.2.1: Certificate #3673
- VMware's OpenSSL FIPS Object Module, version 2.0.20-vmw: Certificate #3857

VMware Cloud Director is in a bundle with the cell management tool (CMT). However, the cell management tool is not FIPS-compliant.

When using the VMware Cloud Director appliance, to configure the appliance to run in FIPS-compliant mode, you must manage both the appliance FIPS mode and the cell FIPS mode.

- Appliance FIPS mode is the mode of the underlying appliance OS, embedded database, and various system libraries.
- Cell FIPS mode is the mode of the VMware Cloud Director cell running on each appliance.

For activating and deactivating FIPS mode on VMware Cloud Director on Linux, see Enable FIPS Mode on the Cells in the Server Group.

Prerequisites

- If metrics collection is activated, verify that the Cassandra certificates follow the X.509 v3 certificate standard and include all the necessary extensions. You must configure Cassandra with the same cipher suites that VMware Cloud Director uses. For information about the allowed SSL ciphers, see Managing the List of Allowed SSL Ciphers.
- Unregister VMware Cloud Director from the vCenter Lookup Service. See Configure vSphere Services in the *VMware Cloud Director Service Provider Admin Portal Guide*.

Procedure

1. From the top navigation bar of the Service Provider Admin Portal, select **Administration**.
2. In the left panel, under **Settings**, select **SSL**.
3. Click **Enable**.
4. To confirm that you want to start the process, click **Enable**.

   When the configuration finishes, VMware Cloud Director displays an `Enable in Progress (Awaiting cells restart)` message, and you can continue to step 5. When you run the API command in step 5, the VMware Cloud Director appliance automatically restarts the cells.
5. To turn on or turn off the appliance FIPS mode, use the VMware Cloud Director appliance API to make a `PUT` request to the `fips/{node_name}` URL. See VMware Cloud Director Appliance API.

   Note You must use the *{node_name}* of the machine processing the `PUT` request.

   Example: Actiavting FIPS Mode

   Request:

   ```
   PUT https://vcloud.example.com:5480/api/1.0.0/fips/{node_name}
   Content-Type: application/json
   ...
   {
       "applianceFips": "ON"
   }
   ```
6. Repeat step 5 for each appliance, for example, primary, standby, and application types.

What to do next

To confirm the state of the cells, you can use the VMware Cloud Director appliance management UI. See View the VMware Cloud Director Appliance FIPS Mode.

View the VMware Cloud Director Appliance FIPS Mode

Starting with version 10.2.2, the VMware Cloud Director appliance can run in FIPS-compliant mode. You can view the appliance and cell FIPS mode.

When using the VMware Cloud Director appliance, to configure the VMware Cloud Director appliance to run in FIPS-compliant mode, you must manage both the appliance FIPS mode and the cell FIPS mode.

- The appliance FIPS mode is the mode of the underlying appliance OS, embedded database, and various system libraries.
- The cell FIPS mode is the mode of the VMware Cloud Director cell running on each appliance.

Table 3-1. FIPS Mode State

Health	Description
	The appliance and cell FIPS modes match. Both modes are either on or off.
	The cell FIPS mode is in a `Pending restart` state. Use the appliance API to activate or deactivate the appliance FIPS mode. Changing the appliance FIPS mode automatically restarts the VMware Cloud Director cell service.
	The VMware Cloud Director appliance cannot determine the cell FIPS mode. The VMware Cloud Director service failing on the appliance can cause the cell FIPS mode to be undetermined.

Prerequisites

Activate or Deactivate FIPS Mode on the VMware Cloud Director Appliance

Procedure

1. Log in as **root** to the appliance management UI at `https://primary_eth1_ip_address:5480`.
2. From the left panel, select **System Configuration**.
3. View the status of the appliance and cell FIPS mode on each node.

Configuring the VMware Cloud Director Appliance SNMP Agent

Starting with VMware Cloud Director 10.2.2, you can configure the VMware Cloud Director appliance SNMP agent to listen for polling requests.

Simple Network Management Protocol (SNMP) is an application layer protocol for management and monitoring of network elements. The VMware Cloud Director appliance includes an SNMP agent that can receive and respond to `GET`, `GETBULK`, and `GETNEXT` requests. The VMware Cloud Director appliance SNMP agent is compatible with all SNMP management services that are compliant with the SNMP standards. You can configure the agent for SNMP v1, v2c, or v3. However, only SNMP v3 offers enhanced security, including cryptographic authentication and encryption.

If there is an existing Net-SNMP agent, before you begin the configuration, consider the following:

- During the upgrade to version 10.2.2 or later, VMware Cloud Director deletes and replaces Net-SNMP with VMware-SNMP.
- You must remove any existing firewall rules that work with Net-SNMP because VMware-SNMP activates and deactivates the polling port when starting and stopping the `snmpd` service.

VMware-SNMP for the VMware Cloud Director appliance supports standard Linux OS management information bases (MIBs) available through the following standard industry MIBs.

- SNMPv2-MIB
- RFC 3418IF-MIB
- RFC 2863IP-MIB
- RFC 4293IP-FORWARD-MIB
- RFC 4292UDP-MIB
- RFC 4113TCP-MIB
- RFC 4022ENTITY-MIB
- RFC 4133HOST-RESOURCES-MIB
- RFC 2790VMWARE-SYSTEM-MIB, REVISION 201008020000Z

Configure a Custom Port for the SNMP Agent

Starting with VMware Cloud Director 10.2.2, if you configure the VMware Cloud Director SNMP agent for polling, it can listen for and respond to requests from SNMP management client systems, such as `GET`, `GETNEXT`, and `GETBULK` requests.

By default, the embedded SNMP agent listens on UDP port 161 for polling requests from management systems. You can use the `vicfg-snmp --port` command to configure an alternative port. To avoid conflicts between the port for the SNMP agent and the ports of other services, reference https://ports.vmware.com/home/VMware-Cloud-Director.

Prerequisites

You must remove any existing firewall rules that work with Net-SNMP because VMware-SNMP activates and deactivates the polling port when starting and stopping the `snmpd` service.

Procedure

1. Log in to the appliance shell as a user with administrative privileges.
2. Deactivate SNMP by running the following command.

   ```
   vicfg-snmp --disable
   ```

3. To change the port that the SNMP agent uses for listening for polling requests, run the following command.

   ```
   vicfg-snmp --port port_number
   ```

Configure the VMware Cloud Director Appliance for SNMP v1 and v2c

Starting with VMware Cloud Director 10.2.2, you can configure VMware Cloud Director appliance for SNMP, by configuring at least one community for the SNMP agent. When you configure the VMware Cloud Director SNMP agent for SNMP v1 and v2c, the agent supports polling.

In SNMP v1 and v2c, community strings are namespaces that contain one or more managed objects. Namespaces can act as a form for authentication but this does not secure the communication. To secure the communication, use SNMP v3.

To enable the VMware Cloud Director appliance SNMP agent to send and receive SNMP v1 and v2c messages, you must configure at least one community for the agent. An SNMP community defines a group of devices and management systems. Only devices and management systems that are members of the same community can exchange SNMP messages. A device or management system can be a member of multiple communities.

Procedure

1. Log in to the appliance shell as a user with administrative privileges.
2. To configure an SNMP community, run the `vicfg-snmp -c` command.

   For example, to configure public, east, and west network operation center communities, run the following command:

   ```
   vicfg-snmp --comunities public,eastnoc,westnoc
   ```

   Every time you specify a community with this command, the settings you specify overwrite the previous configuration. To enter multiple communities, use a comma as a separator.
3. Enable SNMP by running the following command.

   ```
   vicfg-snmp --enable
   ```

Configure the VMware Cloud Director Appliance for SNMP v3

Starting with VMware Cloud Director 10.2.2, you can configure the VMware Cloud Director appliance for SNMP v3. When you configure the SNMP agent for SNMP v3, the agent supports polling and provides stronger security, including cryptographic authentication and encryption.

Configuring the VMware Cloud Director appliance for SNMP v3 consists of three parts.

1 Configuring the SNMP engine ID

2 Configuring SNMP authentication and privacy protocols

3 Configuring SNMP users

Every SNMP v3 agent has an engine ID, which serves as a unique identifier for the agent. The engine ID is used with a hashing function to generate localized keys for authentication and encryption of SNMP v3 messages. If you do not specify an engine ID before you enable the SNMP agent, when you enable the standalone SNMP agent, VMware Cloud Director generates an engine ID.

To ensure the identity of users, you can use authentication. Privacy allows for encryption of SNMP v3 messages to ensure the confidentiality of the data. The privacy protocols provide a higher level of security than is available in SNMP v1 and v2c, which use community strings for security. Both authentication and privacy are optional. However, if you plan to enable privacy, you must enable authentication.

The default value for the authentication and privacy protocols is none.

You can configure up to five users who can access SNMP v3 information. User names must be no more than 32 characters long. While configuring a user, you generate the authentication and privacy hash values based on the authentication and privacy passwords of the user and the engine ID of the SNMP agent. After configuring the users, if you change the engine ID, authentication protocol, or privacy protocol, invalidates the users and you must reconfigure them.

Prerequisites

If you want to configure SNMP authentication and privacy protocols, verify that you know the authentication and privacy passwords for each user that you plan to configure. The passwords must be at least eight characters long.

Procedure

1. Log in to the appliance shell as a user with administrative privileges.
2. Run the `vicfg-snmp --engineid` command to configure the target.

   For example, run the following command:

   ```
   vicfg-snmp --engineid 80001f8880167b18238d613d6000000000
   ```

   Where 80001f8880167b18238d613d6000000000 is the ID, a hexadecimal string between 5 and 32 characters in length.
3. (Optional) To configure the authentication protocol, run the `vicfg-snmp --authentication` command

   For example, run the following command:

   ```
   vicfg-snmp --authentication protocol
   ```

   Where *protocol* must be either **`none`**, for no authentication, **`SHA1`**, **`SHA256`**, **`SHA384`**, or **`SHA512`**. For example, if you want to set the authentication protocol to SHA512, you must run the following command.

   ```
   vicfg-snmp --authentication SHA512
   ```

4 (Optional) To configure the privacy protocol, run the `vicfg-snmp --privacy` command .

For example, run the following command:

```
vicfg-snmp --privacy protocol
```

Where *protocol* must be either **none**, for no privacy, or **AES128**, **AES192**, or **AES256**. For example, if you want to set the privacy protocol to **AES128**, you must run the following command.

```
vicfg-snmp --privacy AES128
```

5 If you are using authentication, privacy, or both, to generate the authentication and privacy hash values for a user, run the following command.

```
vicfg-snmp --hashkey authentication-password privacy-password
```

You must enter the *authentication-password*, the *privacy-password*, or both, depending on your authentication and privacy settings. The passwords must be at least 8 characters long. Make a note of the *authentication-password* and *privacy-password* because you need them for setting up an SNMP client. The output of the command includes the `Authentication localized key` and `Privacy localized key` information.

6 Configure one or more users by running the following command.

You can specify multiple users by adding them as a comma-separated list. You can configure up to five users.

```
vicfg-snmp --users userid/authhash/privhash/security
```

The parameters in the command are as follows.

Parameter	Description
userid	Replace with the user name.
authhash	Replace with the authentication localized key.
privhash	Replace with the privacy localized key.
model	Replace with the level of security enabled for that user, which can be **auth**, for authentication only, **priv**, for authentication and privacy, or **none**, for no authentication or privacy.

For example, if you want to configure a user without security, you can run:

```
vicfg-snmp --users vcd-snmp-user/-/-/none
```

If you want to configure a user with authorization hash, you can run:

```
vicfg-snmp --users vcd-snmp-user/225e07958d3c6af615588db17d61986e69fb7a71/-/auth
```

If you want to configure a user with authorization hash and privacy hash, you can run:

```
vicfg-snmp --users vcd-snmp-user/225e07958d3c6af615588db17d61986e69fb7a71/
da1057af05f67a25a09265a9a2bedb53/priv
```

7 (Optional) If you want to delete one or more users, repeat step 6 with the new user details.

Running `vicfg-snmp --users` again overrides any previous settings.

8 Enable SNMP by running the following command.

```
vicfg-snmp --enable
```

Use `snmpwalk` with VMware Cloud Director SNMP

Starting with VMware Cloud Director 10.2.2, to chain `GETNEXT` requests without entering unique commands for each OID or node within a sub-tree, you can run the `snmpwalk` command.

Prerequisites

- Configure the VMware Cloud Director appliance for Configure the VMware Cloud Director Appliance for SNMP v1 and v2c or Configure the VMware Cloud Director Appliance for SNMP v3.

Procedure

1 On a local machine, verify that you have the `snmpwalk` command installed and install it if necessary.

2 Run the `snmpwalk` command.

```
snmpwalk -v SNMP_version -l security_level -a authorization_procotol -A
authorization_password -x privacy_protocol -X privacy_password -u username host_IP:port
queried_MIB_OID
```

Where `-l` is the security level that you can set to `noAuthNoPriv`, `authNoPriv`, or `authPriv`. For help with the `snmpwalk` command, you can run `-h`.

Example: `snmpwalk` Query

A sample query of the *sysDescr.0* MIB OID can be the following:

```
snmpwalk -v 3 -l authPriv -a SHA512 -A myauthpassword -x AES128 -X myprivpassword -u vcd-snmp-
user 192.168.100.187:10161 sysDescr.0
```

This command returns the following output.

```
SNMPv2-MIB::sysDescr.0 = STRING: VMware-Cloud-Director-Appliance 10.2.2.5553 generic build
17709283 VMware, Inc x86_64
```

Reset the VMware Cloud Director Appliance SNMP Settings

Starting with VMware Cloud Director 10.2.2, you can configure the VMware Cloud Director appliance SNMP agent. To clear all SNMP settings and deactivate the agent, reset the appliance SNMP settings.

Prerequisites

Configure the VMware Cloud Director appliance for Configure the VMware Cloud Director Appliance for SNMP v1 and v2c or Configure the VMware Cloud Director Appliance for SNMP v3.

Procedure

1. Log in to the appliance shell as a user with administrative privileges.
2. To return all SNMP settings to their default values and deactivate the SNMP agent, run the following command.

```
vicfg-snmp --reset
```

Display the VMware Cloud Director Appliance SNMP Settings

Starting with VMware Cloud Director 10.2.2, you can display the SNMP settings, for example, UDP port, communities, V3 users, engine ID, authorization and privacy protocols, and so on.

Prerequisites

Configure the VMware Cloud Director appliance for Configure the VMware Cloud Director Appliance for SNMP v1 and v2c or Configure the VMware Cloud Director Appliance for SNMP v3.

Procedure

1. Log in to the appliance shell as a user with administrative privileges.
2. To display the SNMP settings, run the following command.

```
vicfg-snmp --show
```

Example: Sample `vicfg-snmp --show` Output

The sample output shows that the SNMP agent is enabled for a V3 user with an authorization hash and a privacy hash.

```
Current SNMP agent setting
Enabled : true
UDP port : 161
V1/V2c Communities :
V1 Notification targets :
Notification filter oids:
V3 Notification targets :
V3 Users : vcd-snmp-user 225e07958d3c6af615588db17d61986e69fb7a71
```

```
da1057af05f67a25a09265a9a2bedb53 authPriv
Contact :
Location :
Engine ID : 80001f8880efbab0540a653e6000000000
Auth Protocol : usmHMACSHAAuthProtocol
Priv Protocol : usmAESCfb128PrivProtocol
Log level : warning
Process ID : 15828
Large Storage Support : False
Simple Application Names: False
INFO: listing complete.
```

Edit the DNS Settings of the VMware Cloud Director Appliance

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

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

Prerequisites

To make the changes to the OVF properties permanent, you must use the vSphere UI to change the OVF property values. See the Configure vApp Properties topic in the *vSphere Virtual Machine Administration* guide.

Procedure

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

   a Log in directly or by using an SSH client to the VMware Cloud 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 VMware Cloud Director Appliance Network Interfaces

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

Prerequisites

To make the changes to the OVF properties permanent, you must use the vSphere UI to change the OVF property values. See the Configure vApp Properties topic in the *vSphere Virtual Machine Administration* guide.

Procedure

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

   a Log in directly or by using an SSH client to the VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Appliance

The VMware Cloud 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 VMware Cloud Director Database.

Renew the VMware Cloud Director Appliance Certificates

When you deploy the VMware Cloud 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 VMware Cloud Director cell individually.

The VMware Cloud Director appliance uses two sets of SSL certificates. The VMware Cloud Director service uses one set of certificates for HTTPS and console proxy communications. The embedded PostgreSQL database and the VMware Cloud 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 VMware Cloud 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.
- If FIPS mode is enabled, the **root** password of the appliance must contain 14 or more characters. See Change the VMware Cloud Director Appliance Root Password.

Procedure

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

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

3. Generate new self-signed certificates for the database and appliance management UI or for the HTTPS and console proxy communication, the database, and appliance management UI.
   - Generate self-signed certificates only for the embedded PostgreSQL database and the VMware Cloud Director appliance management UI, run:

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

     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.
   - Generate new self-signed certificates for HTTPS and console proxy communication of VMware Cloud Director in addition to certificates for the embedded PostgreSQL database and the appliance management UI.
     a. Run the following command:

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

b If you are not using CA-signed certificates, run the command to import the newly generated self-signed certificates to VMware Cloud Director.

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

c Restart the VMware Cloud Director service.

```
service vmware-vcd start
```

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 VMware Cloud Director, which are used in 4.

Results

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

The new PostgreSQL certificate is imported to the VMware Cloud Director truststore on other VMware Cloud 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.

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

By default, the embedded PostgreSQL database and the VMware Cloud 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 VMware Cloud Director appliance, it generates self-signed certificates with a validity period of 365 days. The VMware Cloud Director appliance uses two sets of SSL certificates. The VMware Cloud Director service uses one set of certificates for HTTPS and the console proxy communications. The embedded PostgreSQL database and the VMware Cloud 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 VMware Cloud Director truststore on other VMware Cloud Director cells the next time the `appliance-sync` function runs. The operation might take up to 60 seconds.

Replace the Transfer Server Storage for the VMware Cloud Director Appliance

You can change the NFS share for the VMware Cloud Director appliance after deployment.

Procedure

1. Quiesce and stop the `vmware-vcd` service on all appliances in the VMware Cloud Director server group.

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

2. Stop the `appliance-sync.timer` service on all appliances in the server group.

   ```
   systemctl stop appliance-sync.timer
   ```

3. On the primary appliance, copy the data from the old NFS share to the new one.
   a. Create a new NFS share mount point.

      ```
      mkdir /opt/vmware/vcloud-director/data/transfer-new/
      ```

   b. Mount the new NFS server share on the new mount point.

      ```
      mount -t nfs Primary_appliance_IP_address:/data/transfer /opt/vmware/vcloud-director/data/transfer-new
      ```

c Copy the files from the old transfer share to the new transfer share.

Note The time it takes to copy the files depends on the number of catalog items cached in the transfer folder share.

```
cp -R /opt/vmware/vcloud-director/data/transfer/* /opt/vmware/vcloud-director/data/
transfer-new/
```

d When you copy the files successfully, confirm that the contents of the old NFS share are in new NFS share by verifying the contents of `/opt/vmware/vcloud-director/data/transfer-new` or running the following command.

```
diff -r --brief /opt/vmware/vcloud-director/data/transfer/ /opt/vmware/vcloud-director/
data/transfer-new/
```

e Unmount the new NFS share from the temporary mount point.

```
umount /opt/vmware/vcloud-director/data/transfer-new/
```

f Delete the temporary mount point.

```
rmdir /opt/vmware/vcloud-director/data/transfer-new/
```

4 Update the `/etc/fstab` file, replacing the NFS line with the path to the new NFS server.

```
Primary_appliance_IP_address:/data/transfer_appliance /opt/vmware/vcloud-director/data/
transfer/ nfs defaults 0 0
```

5 Unmount the old NFS share.

```
umount /opt/vmware/vcloud-director/data/transfer/
```

6 Mount the new NFS share.

```
mount -a
```

7 Confirm that you mounted the NFS share successfully by verifying that the output of the `mount` command lists the mounted NFS share.

8 Change the ownership of the transfer directory from `root` to `vcloud` using the following command.

```
chown -R vcloud:vcloud /opt/vmware/vcloud-director/data/transfer
```

9 Restart the `appliance-sync.timer` service.

```
systemctl start appliance-sync.timer
```

10 Repeat steps 4 through 9 on all the nodes in the server group.

11 One node at a time, restart the `vmware-vcd` service.

```
systemctl start vmware-vcd
```

12 Verify that `vmware-vcd` works correctly on all nodes in the server group.

Increase the Capacity of the Embedded PostgreSQL Database on a VMware Cloud Director Appliance

If you have insufficient space on the PostgreSQL database disk of a VMware Cloud Director appliance, you can increase the capacity of the embedded PostgreSQL database.

The PostgreSQL database resides on Hard disk 3. It has a default size of 80 GB. The procedure can be done while the appliances are operational.

Important You must increase the capacity of any existing standby appliances before increasing the capacity of the primary appliance.

The PostgreSQL Database disk size on each standby appliance must be the same as the PostgreSQL database disk on the primary appliance.

Prerequisites

- If your VMware Cloud Director environment has standby nodes, identify the standby nodes and the primary node, and begin the procedure from a standby node. For more information on identifying the roles of the nodes, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.
- If your VMware Cloud Director environment consists of only a primary node, run the procedure on the primary node.

Procedure

1 Log in to the vSphere Client to increase the capacity of Hard Disk 3 to the size that you want.

The PostgreSQL database disk size on each standby appliance must be as large as the PostgreSQL database disk on the primary appliance.

a Select the appliance virtual machine that you want to change.

b Select **Actions > Edit Settings**.

c Increase the size of **Hard disk 3** and click **OK**.

The progress of the reconfiguration task appears in the **Recent tasks** pane.

2 Apply the changes to the OS of the appliance node.

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

b To apply the hard disk resizing change to the OS, run the following script.

```
/opt/vmware/appliance/bin/db_diskresize.sh
```

3 If your environment does not consist of only one primary appliance, repeat the procedure for each of the nodes that has a database.

Modify the PostgreSQL Configurations in the VMware Cloud Director Appliance

You can change the VMware Cloud 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 the operation of the cluster requires periodic overwriting of the file and the changes are not persistent.

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.

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.

For more information about the VMware Cloud Director Appliance API, see the VMware Cloud Director Appliance API documentation.

You can unregister the cell during the normal system operation.

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

Procedure

1. To find the name of the standby node that you want to unregister, run the VMware Cloud Director Appliance API method `NODES`.
2. From one of the other nodes, run the VMware Cloud Director Appliance API method `UNREGISTER`.

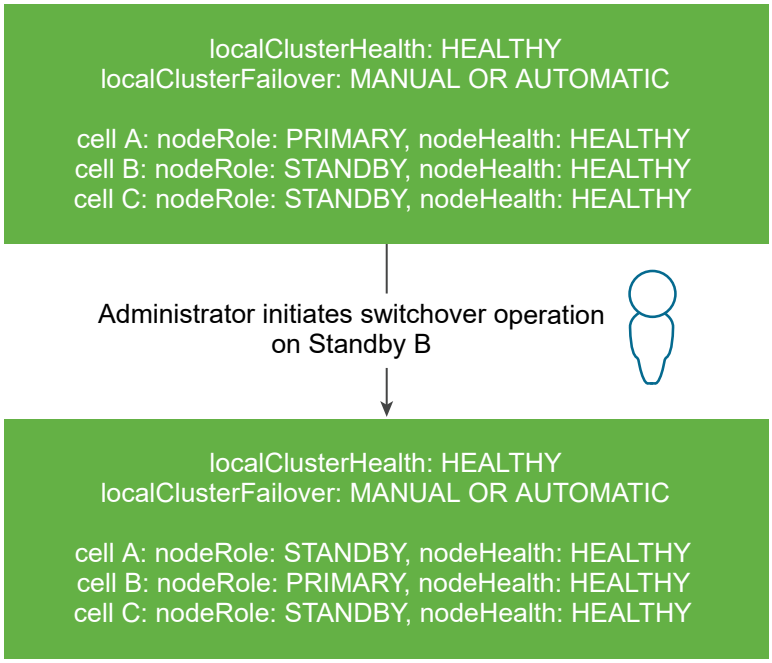
   Where `node-name` is the name of the standby appliance that you want to remove.
3. To verify that the unregistered standby node no longer appears in the database high availability cluster, run the API method `NODES`.

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

You can use the management UI of the VMware Cloud Director appliance to switch the roles of the cells in a database high availability cluster and promote a different cell as the primary.

You can switch the roles of the primary and standby cell by using the VMware Cloud Director appliance management user interface or the VMware Cloud Director appliance API. This procedure describes the steps to do the switchover by using the management UI.

Figure 3-3. Switchover Between the Primary and a Standby Cell



Prerequisites

- Verify that all the nodes in the cluster are healthy and online. See View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

Procedure

1. Quiesce the activities on all VMware Cloud Director cells that are part of the server group or put the cells into maintenance mode.

   The switchover causes the VMware Cloud Director database to be unavailable for 30–60 seconds. To avoid unexpected task failures, you must quiesce the activity on all cells in the cluster.

2. Log in as **root** to the appliance management UI at `https://primary_eth1_ip_address:5480`.

3. In the left panel, select **Embeded Database Availability**.

   You can view the names of the cells, their roles, their status, the name of the cell that the standby cells are following.

4. Verify that the cluster health is `Healthy`.

5. Click the **Switchover** button for the cell that you want to promote as primary and confirm the switchover.

6. When the switchover task completes, restart the scheduler or deactivate maintenance mode for the cells in the cluster.

Subscribe to Events, Tasks, and Metrics by Using an MQTT Client

You can use an MQTT client to subscribe to messages about VMware Cloud Director events and tasks.

MQTT is a lightweight, binary, messaging transport protocol. VMware Cloud Director uses MQTT to publish information about events and tasks to which you can subscribe by using an MQTT client. MQTT messages pass through an MQTT broker which can also store messages in case the clients are not online.

Starting with VMware Cloud Director 10.2.2, you can use an MQTT client to subscribe to metrics.

Prerequisites

- Verify that you have an MQTT client that supports WebSocket.
- Verify that you can add headers to a WebSocket-upgraded request.
- If you want to subscribe to metrics, configure the metrics collection and enable metrics publishing. See Configure Metrics Collection and Publishing.

Procedure

1. Log in to VMware Cloud Director by using the OpenAPI endpoint.
2. To establish a WebSocket connection, set the Sec-WebSocket-Protocol property to `mqtt`, set the client to connect to the `/messaging/mqtt` path, add an authorization header, and follow the standard MQTT connect flow.

   You receive the JWT token from the standard login request to VMware Cloud Director. You can leave the user name and password empty.

   ```
   Sec-WebSocket-Protocol: mqtt
   ```

   ```
   Authorization: Bearer {JWT_token}
   ```

3. Once the connection is established successfully, subscribe to topics through the MQTT client.

   ```
   publish/{user_org_id}/{user_id}
   ```

   ```
   publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
   ```

   Organization administrators can use wildcards to access all organization topics.

   ```
   publish/{user_org_id}/+
   ```

   System administrators can use wildcards to access all topics.

   ```
   publish/#
   ```

4 (Optional) For VMware Cloud Director 10.2.2 or later, subscribe to metrics.

```
metrics/{org_id}/{vApp_id}
```

Only **system administrators** can access the metrics topic.

Auto Scale Groups

Starting with VMware Cloud Director 10.2.2, you can allow tenant users to auto scale applications depending on the current CPU and memory use.

Depending on predefined criteria for the CPU and memory use, tenants can use VMware Cloud Director to automatically scale up or down the number of VMs in a selected scale group. To allow tenants to auto scale applications, you must configure, publish, and grant access to the auto scale solution.

To balance the load of the servers that you configure to run the same application, you can use VMware NSX Advanced Load Balancer (Avi Networks).

Configure and Publish the Auto Scale Plug-in

Before granting access to tenants, you must configure the auto scale groups solution. You can use auto scaling starting from VMware Cloud Director 10.2.2.

1 Log in directly or by using an SSH client to the OS of any of the cells in the cluster as **root**.

2 Enable metric data collection by setting up the metrics collection in a Cassandra database or collect metrics without metrics data persistence.

- Install and Configure a Cassandra Database for Storing Historic Metric Data
- To collect metrics data without data persistence, run the following commands:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.collect.only -v true
```

3 Enable the publishing of metrics.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

4 Create a `metrics.groovy` file in the `/tmp` folder with the following contents.

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
        instance=""
```

```
        minReportingInterval=300
        aggregator="AVERAGE"
    }
}
```

5 Import the file.

```
$VCLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
metrics.groovy
```

6 If you previously configured Cassandra, update the Cassandra schema by providing the correct nodes addresses, database authentication details, port and metrics time to live in days.

```
$VCLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -ttl
TTL_days -update-schema
```

7 If you run the cell with a CA-signed certificate, to enable auto scaling, run the following command.

```
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<username>
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>
```

When running the command from the terminal, escape any special characters using the backslash (\) sign.

8 Restart the cell.

```
service vmware-vcd restart
```

9 Publish the Auto Scale Rights Bundle

Publish the Auto Scale Rights Bundle

If you want tenants to auto scale applications, you must publish the rights bundle to one or more organizations in your system. You can use auto scaling starting from VMware Cloud Director 10.2.2.

Prerequisites

Configure and Publish the Auto Scale Plug-in

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Rights Bundles**.

3 Verify that there are no **Legacy Rights Bundles** for the tenant organizations to which you want to grant access to auto scaling.

4 Select the **vmware:scalegroup Entitlement** bundle, and click **Publish**.

5 To publish the bundle:

   a Select **Publish to Tenants**.

   b Select the organizations to which you want to publish the role.

      - If you want to publish the bundle to all existing and newly created organizations in your system, select **Publish to All Tenants**.
      - If you want to publish the bundle to particular organizations in your system, select the organizations individually.

6 Click **Save**.

What to do next

Add the necessary **VMWARE:SCALEGROUP** rights to the tenant roles that you want to use scale groups. See View and Edit a Global Tenant Role in the *VMware Cloud Director Service Provider Admin Portal Guide*.

Monitoring the VMware Cloud Director Appliance Database Cluster Health

You can monitor your VMware Cloud Director appliance cluster by using the VMware Cloud Director appliance management user interface, the appliance API, or the repmgr open-source tool suite.

You can use the VMware Cloud Director appliance management UI also to view the appliance failover mode. The failover mode indicates whether VMware Cloud Director automatically triggers a database failover if the primary database fails, or the **system administrator** must initiate the failover manually.

If the failover mode is inconsistent across the nodes, the failover mode is `Indeterminate`. The `Indeterminate` mode can lead to inconsistent cluster states between the nodes and nodes following an old primary cell. You must diagnose the problem and remedy the situation manually.

View the VMware Cloud Director Appliance Cluster Health and Failover Mode

You can monitor the cluster status by using the VMware Cloud Director appliance management user interface.

You can view the names of the cells in a cluster, the roles of the cells, the cell status, the name of the cell that the standby cells are following, and the cluster failover mode by using the VMware Cloud Director appliance management UI or the VMware Cloud Director appliance API. This procedure describes the steps to monitor the appliance cluster health in the management UI.

Procedure

1 Log in as **root** to the appliance management UI at `https://primary_eth1_ip_address:5480`.

2 In the left panel, select **Embeded Database Availability**.

You can view the short DNS names of the nodes, their roles, their status, the name of their upstream node, that is, the current primary, and the available actions on the nodes.

In the **Following** column, a question mark (?) in front of the host name indicates that the current primary is unreachable. An exclamation mark (!) in front of the host name indicates that the metadata of the current primary is not updated and might be wrong, or that the node is not attached to the current primary. The problem might occur if you restart the node after a prolonged downtime. If the node cannot attach to the primary, you must unregister it and replace it with a new standby.

3 View the cluster Health.

Cluster Health Status	Description
`Healthy`	The cluster is in a healthy state. The primary and both of the standby cells are online and operational. The VMware Cloud Director UI and API are functional.
`Degraded`	The cluster is in a degraded state. The primary and one of the standby cells are online and operational, but the other standby cell is non-functional. The primary database is functional in this state, but if there is another database failure of either of the operational cells, the primary will become non-functional. The non-functional standby cell must be replaced with a new, functioning standby cell as soon as possible to restore the cluster to a `Healthy` state. The VMware Cloud Director UI and API are functional.
`No_Active_Primary`	There is no operational primary database. If there are two operational standby cells, one of them must be promoted to become the new primary cell. If the environment does not have two operational standby cells, you must diagnose the problem and remedy the situation manually. The VMware Cloud Director UI and API are not available.
`Read_Only_Primary`	There is an online primary database, but it is `Read_Only` because the environment does not have an operational standby cell. Two new standby cells must be deployed. The VMware Cloud Director UI and API are not available.

Cluster Health Status	Description
`Critical_Problem`	The cluster is in an inconsistent state. For example, more than one primary cell is online or a standby cell is following the wrong primary. You must diagnose the problem and remedy the situation manually. This state might affect the VMware Cloud Director UI and API availability.
`SSH_Problem`	The SSH problem indicates that the **postgres** user cannot connect to its peer database nodes over SSH. You must fix this critical problem as soon as possible. See The Cluster Health Indicates an SSH Problem. The VMware Cloud Director UI and API might not be fully functional.

4 View the appliance failover mode.

Failover Mode	Description
Automatic	If a failure of the primary database occurs, VMware Cloud Director automatically triggers a database failover.
Manual	If a failure of the primary database occurs, you must initiate a database failover using the VMware Cloud Director appliance management UI or failover API.
Indeterminate	Failover mode is not consistent across all the nodes of the cluster. You must diagnose the problem and remedy the situation. By using the VMware Cloud Director appliance API, reset the `FailoverMode` to either `Manual` or `Automatic`. See the *Failovermode* information in the *VMware Cloud Director Appliance API Schema Reference*.

View the VMware Cloud Director Appliance Service Status

You can monitor the status of the VMware Cloud Director appliance services by using the VMware Cloud Director appliance management user interface.

On the services tab, you can monitor the `vmware-vcd`, `vpostgres`, and `appliance-sync.timer` services for primary and standby appliances and the `vmware-vcd` and `appliance-sync.timer` services for application cells.

The `appliance-sync.timer` service periodically runs the `appliance-sync.service` which shares relevant information between all nodes in the database HA cluster or VMware Cloud Director server group. `appliance-sync.service` runs a periodic check and sync of needed files for the VMware Cloud Director appliance functionality by reading and writing the configuration files of the appliances in the appliance group. The healthy states of the timer are `waiting` and `running`.

Procedure

1 Log in as **root** to the appliance management UI at `https://primary_eth1_ip_address:5480`.

2 In the left panel, select the **Services** tab.

3 View the status of the VMware Cloud Director services.

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 for the primary provides information on the node, PostgreSQL version, and replication details. For example:

```
Node "bos1-vcloud-static-161-5":
        PostgreSQL version: 10.9
        Total data size: 81 MB
        Conninfo: host=172.18.36.193 user=repmgr dbname=repmgr connect_timeout=2
        Role: primary
        WAL archiving: off
        Archive command: (none)
        Replication connections: 2 (of maximal 10)
        Replication slots: 0 physical (of maximal 10; 0 missing)
        Replication lag: n/a
```

The system output for a standby node provides information on the node, PostgreSQL version, replication details and an upstream node. For example:

```
Node "bos1-vcloud-static-161-49":
    PostgreSQL version: 10.9
    Total data size: 83 MB
    Conninfo: host=172.18.36.191 user=repmgr dbname=repmgr connect_timeout=2
    Role: standby
    WAL archiving: off
    Archive command: (none)
    Replication connections: 0 (of maximal 10)
    Replication slots: 0 physical (of maximal 10; 0 missing)
    Upstream node: bos1-vcloud-static-161-48 (ID: 683)
    Replication lag: 0 seconds
    Last received LSN: 2/D863B4E0
    Last replayed LSN: 2/D863B4E0
```

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.	`select* from pg_stat_replication;`
Run a query on a standby node.	`select* from pg_stat_wal_receiver;`

Check the Status of VMware Cloud Director Services

You can use the management UI of the VMware Cloud Director appliance to view the status of the VMware Cloud Director services for the cell in which you are logged in.

Procedure

1 Log in as **root** to the appliance management UI at `https://primary_eth1_ip_address:5480`.

2 To view the status of the services, from the left panel, select **Services**.

If the VMware Cloud Director appliance is working properly, the `vmware-vcd` and `vpostgres` services are running.

What to do next

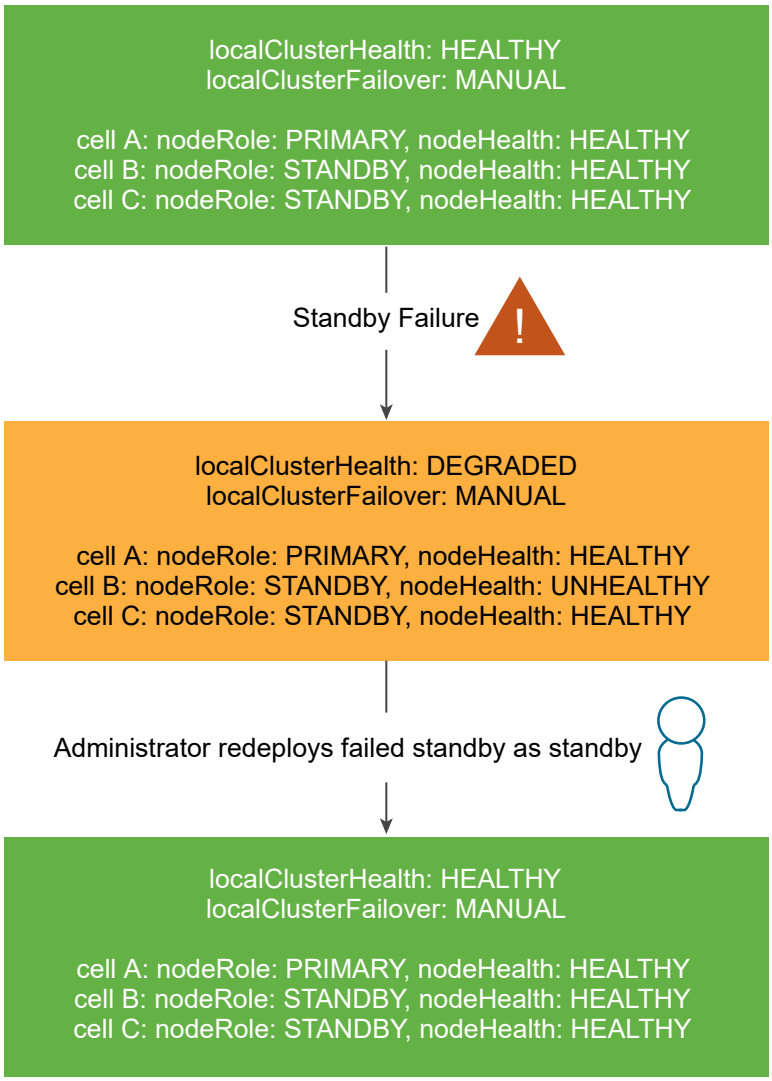
If you need to check the status of the `repmgrd` service for debugging purposes, you must use the VMware Cloud Director Appliance API.

VMware Cloud Director Appliance Database Cluster Recovery

If there is a failure with the database or one of the VMware Cloud Director nodes, you can recover your database cluster.

If a cell in the database high availability cluster fails, the cluster health status indicates what the failure is and how you can resolve the issue. For example, the `Degraded` cluster health indicates a failure with a standby cell. A system administrator must redeploy the failed cell.

Figure 3-4. Recover from a Standby Cell Failure



If a primary cell in the database high availability cluster fails, the cluster health can change to `No_Active_Primary`, which indicates that a system administrator must repair the failed primary cell.

Recover from a Primary Cell Failure in a High Availability Cluster

If the primary cell is not running properly, to recover the VMware Cloud Director database, one of the standby cells must become the new primary cell and you must deploy a new standby. Depending on the failure mode, the VMware Cloud Director appliance automatically promotes a standby cell as the new primary or you must promote it manually.

Depending on the failover mode of the VMware Cloud Director appliance, there are two different workflows for recovering from a primary cell failure. You can use these workflows to reuse the IP addresses and hostname of the failed primary when you deploy the new standby.

Recovery Workflow for Manual Failover Mode

If the primary cell is in the `Not reachable` or `Failed` state and the two standby cells are in the `Running` state, you can recover from the failure by using the appliance HTML5 user interface and the VMware Cloud Director appliance API.

To view the state of the cells in the cluster, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

1 By using the call management tool, if possible, shut down the VMware Cloud Director process. From the failed primary cell, run the following command

```
/opt/vmware/vcloud-director/bin/cell-management-tool  -u <sysadmin user> cell --shutdown
```

2 Power off the failed primary VM.

3 Promote a standby cell to become the new primary.

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

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

   The management UI shows two cells with the `primary` role. The original primary has a `failed` status and the new primary has a `running` status. The cluster health is `Degraded`.

4 From any cell other than the failed primary, using the appliance API `Unregister` method, remove the failed primary appliance from the repmgr high availability cluster. See the VMware Cloud Director Appliance API documentation.

5 Remove the failed primary appliance from the VMware Cloud Director server group.

   a Log in as an **administrator** to the Service Provider Admin Portal.

   b From the top navigation bar, under **Resources**, select **Cloud Resources**.

   c In the left panel, click **Cloud Cells**.

d Select the inactive cell and click **Unregister**.

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 use the vSphere Client to delete it.

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

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

8 If the VMware Cloud Director appliance FIPS mode was on before the restore, you must set it again by using the VMware Cloud Director appliance API.

The cell FIPS mode restores automatically.

Recovery for Automatic Failover Mode

If the primary is in the `Failed` state, VMware Cloud Director automatically promotes a standby cell as the new running primary but the cluster is in the `Degraded` state because there is only one running standby cell. You can recover from the failure by using the HTML5 user interface and the VMware Cloud Director appliance API.

To view the state of the cells in the cluster, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

1 If possible, by using the call management tool, shut down the VMware Cloud Director process. From the failed primary cell, run the following command

```
/opt/vmware/vcloud-director/bin/cell-management-tool  -u <sysadmin user> cell --shutdown
```

2 Power off the failed primary VM.

The management UI shows two cells with the `primary` role. The original primary has a `failed` status and the new primary has a `running` status. The cluster health is `Degraded`.

3 From any cell other than the failed primary, by using the appliance API `Unregister` method, remove the failed primary appliance from the repmgr high availability cluster. See the VMware Cloud Director Appliance API documentation.

4 Remove the failed primary appliance from the VMware Cloud Director server group.

a Log in as an **administrator** to the Service Provider Admin Portal.

b From the top navigation bar, under **Resources**, select **Cloud Resources**.

c In the left panel, click **Cloud Cells**.

d Select the inactive cell and click **Unregister**.

5 If you want to reuse the IP address and hostname of the failed primary, ensure that the failed primary appliance is powered off or use the vSphere Client to delete it.

6 Deploy a new standby appliance. You can Start the VMware Cloud Director Appliance Deployment or Deploying the VMware Cloud Director Appliance by Using VMware OVF Tool. After deploying the new standby, the cluster health must be `Healthy`.

7 From any cell other than the failed primary cell, use the appliance API `Failover` method to reset the cluster failover mode to `Automatic`. See the VMware Cloud Director Appliance API documentation.

8 If the VMware Cloud Director appliance FIPS mode was on before the restore, you must set it again by using the VMware Cloud Director appliance API.

   The cell FIPS mode restores automatically.

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 `Not reachable` or `Failed` state, you can deploy a new cell. To view the state of the cells in the cluster, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

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 VMware Cloud 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 From any cell other than the failed standby cell, by using the appliance API `Unregister` method, remove the failed standby cell from the repmgr high availability cluster. See the VMware Cloud Director Appliance API documentation.

4 Use the Service Provider Admin Portal to remove the failed standby appliance from the VMware Cloud Director server group.

   a From the top navigation bar, under **Resources**, select **Cloud Resources**.

   b In the left panel, click **Cloud Cells**.

   c Select an inactive cell and click **Unregister**.

5 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.

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

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

7 To reset the cluster failover mode to `Automatic`, from any cell other than the failed standby cell, use the appliance API `Failover` method. See the VMware Cloud Director Appliance API documentation.

For more information about the automatic failover mode, see Automatic Failover of the VMware Cloud Director Appliance.

8 If the VMware Cloud Director appliance FIPS mode was on before the restore, you must set it again by using the VMware Cloud Director appliance API.

The cell FIPS mode restores automatically.

Unregister a Failed Primary or Standby Cell in a Database High Availability Cluster

If the primary or standby node in your database high availability cluster fails, you can use the VMware Cloud Director API to unregister the failed node to remove it from the cluster and avoid inconsistent cluster status data.

For more information about using the VMware Cloud Director API, see the `UNREGISTER` API method in the VMware Cloud Director Appliance API documentation at https://developer.vmware.com/.

Prerequisites

- Verify that the node you want to unregister is inactive and make a note of its name. For information about the status of the cells and the name of the cell the standby cells are following, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.
- If you want to unregister a primary node, verify that the failed primary is inactive and without any following standby nodes, and promote a new primary.

Procedure

- To remove the inactive node, make a DELETE request on an active node on which to run the command.

```
DELETE https://<Active _Node_FQDN>:5480/api/1.0.0/nodes/<Inactive_Node_Name>
```

Troubleshooting the Appliance

If the VMware Cloud 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 VMware Cloud Director logs. For more information about collecting diagnostic information for VMware Cloud 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.

Examine the Log Files in the VMware Cloud Director Appliance

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

Procedure

1. Log in directly or by using an SSH client to the VMware Cloud 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 VMware Cloud Director Cell Fails to Start After the Appliance Deployment

You deployed the VMware Cloud Director appliance successfully, but the VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.

Note If your cluster is configured for automatic failover, after you deploy one or more additional cells, you must use the Appliance API to reset the cluster failover mode to `Automatic`. See the VMware Cloud Director Appliance API. The default failover mode for new cells is `Manual`. If the failover mode is inconsistent across the nodes of the cluster, the cluster failover mode is `Indeterminate`. The `Indeterminate` mode can lead to inconsistent cluster states between the nodes and nodes following an old primary cell. To view the cluster failover mode, see View the VMware Cloud Director Appliance Cluster Health and Failover Mode.

Solution

1. Log in directly or by using an SSH client to the VMware Cloud 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 .

Recovering After NFS Validation Fails During the Initial Appliance Configuration

If the shared storage validation fails during the initial VMware Cloud Director appliance configuration, the deployer displays error messages that you can use to remediate the issue.

Problem

During the VMware Cloud Director appliance deployment, the deployer displays an error message referring to the NFS share.

Cause

If you do not prepare the transfer server storage for the VMware Cloud Director, the NFS validation during deployment fails.

Solution

Version	Error	Action
10.2	`/opt/vmware/vcloud-director/data/transfer/xyz is owned by an unknown user with UID 999; expected 1003`	Verify the user ID configuration of the **vcloud** user on the NFS server. The **vcloud** user ID must be with the same value on the NFS server and the appliance.
10.2	`/opt/vmware/vcloud-director/data/transfer/xyz is owned by an unknown user with GID 999; expected 1002`	Verify the group ID configuration of the **vcloud** user on the NFS server. The **vcloud** user ID must be with the same value on the NFS server and the appliance.
10.2	`Unable to touch file on transfershare`	Determine why the appliance cannot write on the mounted NFS share. To confirm why it is not writeable, try mounting the NFS share using another Linux machine.
10.2	`Timeout encountered during /usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test. Duration: 5 seconds`	Determine why this appliance cannot mount the specified NFS share within 5 seconds. To confirm if the NFS share cannot be mounted in a timely manner, try mounting it using another Linux machine. Alternatively, verify the NFS server export settings for this NFS share.
10.2	`Error encountered during /usr/bin/mount -t nfs 10.150.170.3:/data/transfer /opt/vmware/vcloud-director/data/nfs-test`	Determine why this appliance cannot mount the specified NFS share . To confirm if the NFS share cannot be mounted, try mounting it using another Linux machine. Alternatively, verify the NFS server export settings for this NFS share.
10.2	`Transfer share directory does not exist: /opt/vmware/vcloud-director/data/transfer`	The transfer share directory or mount point does not exist. Create that directory.
10.2	`Unexpected permissions on file /opt/vmware/vcloud-director/data/transfer/xyz while performing operation: touch xyz. Expected: root root 644. Found: root, root, 600`	Determine why the file owner, group, or permissions defer from the expected values after performing the specified operation on the NFS transfer share and correct the problem.
10.2	`NFS server clock is out of sync with respect to the appliance clock. Time difference is: 3 minutes, 12 seconds`	Verify the time settings on the NFS server and appliance. If either or both are not accurate, set them to the correct time and ensure they are synchronized using NTP.

Version	Error	Action
10.2	`Unexpected permissions on file /opt/vmware/vcloud-director/data/transfer/xyz while performing operation: chmod xyz. Expected: root root 750. Found: root, root, 700`	Determine why the file owner, group, or permissions defer from the expected values after performing the specified operation on the NFS transfer share and correct the problem.
10.2	`Unexpected permissions on file /opt/vmware/vcloud-director/data/transfer/xyz while performing operation: chown xyz. Expected: root root 750. Found: root, root, 700`	Determine why the file owner, group, or permissions defer from the expected values after performing the specified operation on the NFS transfer share and correct the problem.
10.2 and later	`Invalid or missing command arguments. usage: nfsValidate` *`nfs_mount_string`*	The JSON request body cannot be parsed. Provide a valid JSON request body.
10.2 and later	`Empty nfs_mount string`	The NFS mount string is not in the request body. Provide an NFS mount string argument.
10.2 and later	`Invalid nfs_mount string:` *`nfs_mount_string_argument`*	Change the NFS mount string to the valid format *IP_address:path*
10.2 and later	`Invalid cell type:` *`cell_type_string`*	The cell type must be `primary`, `standby`, or `cell`. If the OVF parameter is not equal to any of these values, verify the appliance configuration.
10.2 and later	`Prerequisite OS configuration was not completed`	The `/opt/vmware/appliance/etc/os-configuration-completed` file is missing from the appliance. Configure the operating system.
10.2 and later	`Cloud Director appliance system setup already complete.`	The `/opt/vmware/appliance/etc/vcd-configuration-completed` file was found on the appliance. The cloud directory setup is already complete, and you must not run this script.
10.2 and later	`The 10.150.170.3:/data/transfer/cells directory already exists. The primary appliance requires that this be removed.`	This directory must not exist on the primary appliance. The directory exists on the NFS server and you must remove it.
10.2 and later	`The 10.150.170.3:/data/transfer/appliance-nodes directory already exists. The primary appliance requires that this be removed.`	This directory must not exist on the primary appliance. The directory exists on the NFS server and you must remove it.

Version	Error	Action
10.2 and later	`responses.properties file already exists on transfer share. The primary appliance requires that this be removed.`	On the primary appliance, the `responses.properties` files must not exist, and you must remove them.
10.2 and later	`responses.properties file does not exist on transfer share. This should already exist on a standby or cell appliance.`	On a standby or cell appliance, the `responses.properties` file must exist. The primary appliance might not be configured yet. You must configure the primary appliance before configuring additional cells.
10.2 and later	`nfsValidate can not be run while system setup is in progress.`	Wait for the system setup to complete before attempting to run `nfsValidate`.
10.2 and later	`Unable to create tmp directory for use by this script: /opt/vmware/vcloud-director/data/nfs-test`	Verify file system permissions to determine why this directory cannot be created.
10.2.1	`Unable to create file on provided NFS share. It may not be writeable. This may be due to the exported NFS filesystem being read-only or no_root_squash was not specified`	Determine why the appliance cannot write on the mounted NFS share. To confirm why it is not writeable, try mounting the NFS share using another Linux machine.
10.2.1	`Unable to chmod file on provided transfershare`	Determine why the appliance cannot change the access permissions of file system objects on the mounted NFS share. Try mounting the NFS share using another Linux machine.
10.2.1	`Unable to chown file on provided transfershare`	Determine why the appliance cannot change the owner of file system objects on the mounted NFS share. Try mounting the NFS share using another Linux machine.
10.2.1	`Timeout encountered during mount`	Determine why this appliance cannot mount the specified NFS share within 5 seconds. To confirm if the NFS share cannot be mounted in a timely manner, try mounting it using another Linux machine. Alternatively, verify the NFS server export settings for this NFS share.

Version	Error	Action
10.2.1	Error encountered during mount	Determine why this appliance cannot mount the specified NFS share . To confirm if the NFS share cannot be mounted, try mounting it using another Linux machine. Alternatively, verify the NFS server export settings for this NFS share.
10.2.1	`Provided NFS share is owned by an unknown user with UID 123; expected rootProvided NFS share is owned by an unknown group with GID 456; expected root`	Determine why the expected file owner, group, or both defer from the expected values after performing the specified operation on the NFS transfer share and correct the problem.
10.2.1	`Unexpected ownership and/or permissions on provided NFS share. Expected: root:root with mode: 750. Found: root:root with mode 777`	Determine why some or all of the expected values for file owner, group, and mode are not as expected after performing the specified operation on the NFS transfer share. Correct the problem.
10.2.1	`NFS server clock is out of sync with respect to the appliance clock. Time difference is: 1:55:14.603510`	Verify the time settings on the NFS server and appliance. If either or both are not accurate, set them to the correct time and ensure they are synchronized using NTP.

Reconfiguring the VMware Cloud Director Service Fails When Migrating or Restoring to VMware Cloud Director Appliance

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

Problem

During the procedure for migrating or restoring VMware Cloud Director to a new VMware Cloud Director appliance environment, you run the `configure` command to reconfigure the VMware Cloud 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.

A VMware Cloud Director Appliance Standby Node Becomes Unreachable

VMware Cloud Director maintains synchronous streaming replication between the nodes. If a standby node becomes unreachable, you must determine the cause and resolve the problem.

Problem

The VMware Cloud Director appliance management UI shows the cluster health as `DEGRADED` and the status of one of the standby nodes is `? unreachable`.

The `/nodes` API returns information that the `localClusterHealth` is `DEGRADED`, the node `status` is `? unreachable`, and the `nodeHealth` is `UNHEALTHY`.

For example, the `/nodes` API might return the following information for the node.

```
{
    "localClusterFailover": "MANUAL",
    "localClusterHealth": "DEGRADED",
    "localClusterState": [
        {
            "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover = manual",
                "mode": "MANUAL",
                "repmgrd": {
                    "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
                    "status": "NOT APPLICABLE"
                }
            },
            "id": primary_node_ID,
            "location": "default",
            "name": "primary_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "PRIMARY",
            "role": "primary",
            "status": "* running",
            "upstream": ""
        },
        {
            "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover state unknown - unable to ssh to failed or unreachable
node",
                "mode": "UNKNOWN",
                "repmgrd": {
                    "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = n/a",
                    "status": "UNKNOWN"
                }
            },
```

```
            "id": unreachable_standby_node_ID,
            "location": "default",
            "name": "unreachable_standby_host_name",
            "nodeHealth": "UNHEALTHY",
            "nodeRole": "STANDBY",
            "role": "standby",
            "status": "? unreachable",
            "upstream": "primary_host_name"
        },
        {
            "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover = manual",
                "mode": "MANUAL",
                "repmgrd": {
                    "details": "On node running_standby_node_ID (running_standby_host_IP):
repmgrd = not applicable",
                    "status": "NOT APPLICABLE"
                }
            },
            "id": running_standby_node_ID,
            "location": "default",
            "name": "running_standby_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "STANDBY",
            "role": "standby",
            "status": "running",
            "upstream": "primary_host_name"
        }
    ],
    "warnings": [
        "unable to connect to node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID)",
        "node \"unreachable_standby_host_name\" (ID: unreachable_standby_node_ID) is
registered as an active standby but is unreachable"
    ]
}
```

Cause

To ensure data integrity, the PostgreSQL database uses Write-Ahead Logging (WAL). The primary node streams the WAL constantly to the active standby nodes for replication and recovery purposes. The standby nodes process the WAL when they receive it. If a standby node is unreachable, it stops receiving the WAL and cannot be a candidate for promotion to become a new primary.

Solution

- Verify that the virtual machine of the unreachable standby node is running.
- Verify that the network connection to the standby node is working.

- Verify that there is no SSH problem that might prevent the standby node from communicating with the other nodes.
- Verify that the vpostgres service on the standby node is running.

What to do next

To verify that there are no network or SSH problems, see Check the Connectivity Status of a Database High Availability Cluster.

A VMware Cloud Director Appliance Standby Node Becomes Unattached

VMware Cloud Director maintains synchronous streaming replication between the nodes. If a standby node becomes unattached, you must determine the cause and resolve the problem.

Problem

The VMware Cloud Director appliance management UI shows the cluster health as `DEGRADED`, the status of one of the unattached standby nodes is `running`, and there is an exclamation point (!) before the name of the upstream node for the standby.

The PostgreSQL log shows that the primary deleted a WAL segment.

```
2020-10-08 04:10:50.064 UTC [13390] LOG:  started streaming WAL from primary at 21/80000000
on timeline 17
2020-10-08 04:10:50.064 UTC [13390] FATAL:  could not receive data from WAL stream: ERROR:
requested WAL segment 000000110000002100000080 has already been removed
2020-10-08 04:10:55.047 UTC [13432] LOG:  started streaming WAL from primary at 21/80000000
on timeline 17
2020-10-08 04:10:55.047 UTC [13432] FATAL:  could not receive data from WAL stream: ERROR:
requested WAL segment 000000110000002100000080 has already been removed
```

The `/nodes` API returns information that the `localClusterHealth` is `DEGRADED`, the node `status` is `running`, the `nodeHealth` is `HEALTHY`. There is an exclamation point (!) before the name of the upstream node for the standby and the `/nodes` API returns a warning that the standby is not attached to its upstream node.

For example, the `/nodes` API might return the following information for the node.

```
{
    "localClusterFailover": "MANUAL",
    "localClusterHealth": "DEGRADED",
    "localClusterState": [
        {
            "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover = manual",
                "mode": "MANUAL",
                "repmgrd": {
                    "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
```

```
                    "status": "NOT APPLICABLE"
                }
            },
            "id": primary_node_ID,
            "location": "default",
            "name": "primary_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "PRIMARY",
            "role": "primary",
            "status": "* running",
            "upstream": ""
        },
        {
            "connectionString": "host=unattached_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover = manual",
                "mode": "MANUAL",
                "repmgrd": {
                    "details": "On node unattached_standby_node_ID
(unattached_standby_host_name): repmgrd = not applicable",
                    "status": "NOT APPLICABLE"
                }
            },
            "id": unattached_standby_node_ID,
            "location": "default",
            "name": "unattached_standby_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "STANDBY",
            "role": "standby",
            "status": "running",
            "upstream": "! upstream_host_name"
        },
        {
            "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover = manual",
                "mode": "MANUAL",
                "repmgrd": {
                    "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = not applicable",
                    "status": "NOT APPLICABLE"
                }
            },
            "id": running_standby_node_ID,
            "location": "default",
            "name": "running_standby_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "STANDBY",
            "role": "standby",
            "status": "running",
            "upstream": "upstream_host_name"
        }
    ],
```

```
    "warnings": [
        "node \"unattached_standby_host_name\" (ID: unattached_standby_node_ID) is not
attached to its upstream node \"upstream_host_name\" (ID: upstream_node_id)"
    ]
}
```

If a standby node becomes unattached, you must reattach it as soon as possible. If the node stays unattached for too long, it might fall behind in processing the continuously streaming WAL records from the primary to such an extent that it might not be possible for it to resume replication.

Cause

To ensure data integrity, the PostgreSQL database uses Write-Ahead Logging (WAL). The primary node streams the WAL constantly to the active standby nodes for replication and recovery purposes. The standby nodes process the WAL when they receive it. If a standby node becomes unattached, it stops receiving the WAL and cannot be a candidate for promotion to become a new primary.

Solution

1. Deploy a new standby node.
2. Unregister the unattached standby node.

What to do next

See Recover from a Standby Cell Failure in a High Availability Cluster.

The Cluster Health Indicates an SSH Problem

In a VMware Cloud Director appliance deployment with database HA configuration, the **postgres** user cannot connect to its peer database nodes over SSH.

Problem

When there is an SSH problem between the database nodes, VMware Cloud Director shows the `localClusterHealth` as `SSH_PROBLEM`. You must fix this critical problem as soon as possible.

You can view the `localClusterHealth` by using the VMware Cloud Director appliance management user interface or run the `/nodes` VMware Cloud Director appliance API. See the VMware Cloud Director Appliance API documentation.

When you run the `/nodes` API on a peer node of the one with the SSH problem, the `/nodes` API returns information that the `localClusterHealth` is `SSH_PROBLEM`, the `localClusterFailover` is `INDETERMINATE`. The failover mode is `INDETERMINATE` because the node on which you run the `/nodes` API cannot connect to one of its peer nodes over SSH. The `"details"` in the `"failover"` output part of the response body for the node with SSH problem displays: `ssh failed. command: ssh unreachable_standby_host_IP /usr/bin/grep failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf`.

For example, if a standby node has an SSH problem and you run `GET https://primary_host_IP:5480/api/1.0.0/nodes`, the `/nodes` API might return the following information.

```
{
    "localClusterFailover": "INDETERMINATE",
    "localClusterHealth": "SSH_PROBLEM",
    "localClusterState": [
        {
            "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover = manual",
                "mode": "MANUAL",
                "repmgrd": {
                    "details": "On node primary_node_ID (primary_host_name): repmgrd = not
applicable",
                    "status": "NOT APPLICABLE"
                }
            },
            "id": primary_node_ID,
            "location": "default",
            "name": "primary_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "PRIMARY",
            "role": "primary",
            "status": "* running",
            "upstream": ""
        },
        {
            "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover = manual",
                "mode": "MANUAL",
                "repmgrd": {
                    "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = not applicable",
                    "status": "NOT APPLICABLE"
                }
            },
            "id": running_standby_node_ID,
            "location": "default",
            "name": "running_standby_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "STANDBY",
            "role": "standby",
            "status": "running",
            "upstream": "primary_host_name"
        },
        {
            "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "ssh failed. command: ssh unreachable_standby_host_IP /usr/bin/
```

```
grep failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
                "mode": "UNKNOWN",
                "repmgrd": {
                    "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = not running",
                    "status": "NOT RUNNING"
                }
            },
            "id": unreachable_standby_node_ID,
            "location": "default",
            "name": "unreachable_standby_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "STANDBY",
            "role": "standby",
            "status": "running",
            "upstream": "primary_host_name"
        }
    ],
    "warnings": []
}
```

If you run `GET https://unreachable_standby_host_IP:5480/api/1.0.0/nodes`, because the node is untrusted, the `localClusterFailover` and `localClusterState` information might not be correct. The `/nodes` API returns warning messages that the *unreachable_standby_host_name* is unable to connect to its peer nodes.

For example, the `/nodes` API might return the following information.

```
{
    "localClusterFailover": "MANUAL",
    "localClusterHealth": "SSH_PROBLEM",
    "localClusterState": [
        {
            "connectionString": "host=primary_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "ssh failed. command: ssh primary_host_IP /usr/bin/grep
failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
                "mode": "UNKNOWN",
                "repmgrd": {
                    "details": "On node primary_node_ID (primary_host_name): repmgrd = n/a",
                    "status": "UNKNOWN"
                }
            },
            "id": primary_node_ID,
            "location": "default",
            "name": "primary_host_name",
            "nodeHealth": "UNHEALTHY",
            "nodeRole": "PRIMARY",
            "role": "primary",
            "status": "? running",
            "upstream": ""
        },
        {
```

```
            "connectionString": "host=running_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "ssh failed. command: ssh running_standby_host_IP /usr/bin/grep
failover=manual /opt/vmware/vpostgres/10/etc/repmgr.conf",
                "mode": "UNKNOWN",
                "repmgrd": {
                    "details": "On node running_standby_node_ID (running_standby_host_name):
repmgrd = n/a",
                    "status": "UNKNOWN"
                }
            },
            "id": running_standby_node_ID,
            "location": "default",
            "name": "running_standby_host_name",
            "nodeHealth": "UNHEALTHY",
            "nodeRole": "STANDBY",
            "role": "standby",
            "status": "? running",
            "upstream": "primary_host_name"
        },
        {
            "connectionString": "host=unreachable_standby_host_IP user=repmgr dbname=repmgr
connect_timeout=2",
            "failover": {
                "details": "failover = manual",
                "mode": "MANUAL",
                "repmgrd": {
                    "details": "On node unreachable_standby_node_ID
(unreachable_standby_host_name): repmgrd = not applicable",
                    "status": "NOT APPLICABLE"
                }
            },
            "id": unreachable_standby_node_ID,
            "location": "default",
            "name": "unreachable_standby_host_name",
            "nodeHealth": "HEALTHY",
            "nodeRole": "STANDBY",
            "role": "standby",
            "status": "running",
            "upstream": "? primary_host_name"
        }
    ],
    "warnings": [
        "unable to connect to node \"primary_host_name\" (ID: primary_node_ID)",
        "unable to connect to node \"running_standby_host_name\" (ID:
running_standby_node_ID)",
        "unable to connect to node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID)'s upstream node \"primary_host_name\" (ID: primary_node_ID)",
        "unable to determine if node \"unreachable_standby_host_name\" (ID:
unreachable_standby_node_ID) is attached to its upstream node \"primary_host_name\" (ID:
primary_node_ID)"
    ]
}
```

Cause

VMware Cloud Director stores the SSH certificates of the **postgres** user on the NFS shared transfer server storage. All database nodes must have access to the shared transfer server storage. If a database node becomes untrusted, that is, the SSH certificates of the **postgres** user are either no longer valid or accessible, that node is unable to run commands on its peer nodes by using an SSH client. The VMware Cloud Director appliance must have this capability to perform properly when in HA mode.

Solution

1. Determine whether there is a connectivity problem between the nodes and correct the problem. See Check the Connectivity Status of a Database High Availability Cluster.
2. Verify that the `appliance-sync.timer` service is running on the nodes that have the SSH problem by running the following command.

   ```
   systemctl status appliance-sync.timer
   ```

   For example, the command might return:

   ```
   * appliance-sync.timer - Periodic check and sync of needed files for Cloud Appliance
   functionality
      Loaded: loaded (/lib/systemd/system/appliance-sync.timer; enabled; vendor preset:
   enabled)
      Active: active (waiting) since Sat 2020-09-05 23:22:49 UTC; 1 months 9 days ago

   Warning: Journal has been rotated since unit was started. Log output is incomplete or
   unavailable.
   ```

3. If the status of the `appliance-sync.timer` service is not `Active`, restart the service by running the following command.

   ```
   systemctl start appliance-sync.timer
   ```

4. Wait for approximately 90 seconds and verify that the cluster health is `HEALTHY` by using the VMware Cloud Director management UI or call the `/nodes` API.

Using the Log Files to Troubleshoot VMware Cloud Director Updates and Patches

You can examine the log files for errors and warnings when you apply patches to the VMware Cloud 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 VMware Cloud 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 VMware Cloud Director Updates Fails

When you are checking for updates to the VMware Cloud Director appliance, running the `vamicli update --check` command might fail.

Problem

During the procedure of applying a patch to the VMware Cloud 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 VMware Cloud Director Fails

When you are installing the latest updates to the VMware Cloud Director appliance, running the `vamicli update --install latest` command might fail.

Problem

During the procedure of applying a patch to the VMware Cloud 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
```

Installation, Upgrade, and Administration of VMware Cloud Director on Linux

4

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

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

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

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

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

This chapter includes the following topics:

Configuration Planning

vSphere provides storage, compute, and networking capacity to VMware Cloud Director. Before you begin the installation, consider how much vSphere and VMware Cloud 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 VMware Cloud Director cell for each vCenter Server system that you want to make accessible in your cloud.
- Be sure that all target VMware Cloud Director Linux servers meet at least the minimum requirements for memory and storage detailed in *VMware Cloud Director Release Notes*.
- If you plan to install VMware Cloud Director on Linux, configure the VMware Cloud Director database as described in Configure an External PostgreSQL Database for VMware Cloud Director on Linux.

Preparing for the VMware Cloud Director Installation

Before you install VMware Cloud Director on a Linux server, you must prepare your environment.

Configure an External PostgreSQL Database for VMware Cloud Director on Linux

The VMware Cloud Director cells use a database to store shared information. Before you install VMware Cloud Director on Linux, you must install and configure a PostgreSQL database instance and create the VMware Cloud Director database user account.

PostgreSQL databases have specific configuration requirements when you use them with VMware Cloud Director.

You must create a separate, dedicated database schema for VMware Cloud Director to use. VMware Cloud Director cannot share a database schema with any other VMware product.

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

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

Prerequisites

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

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

Preparing the Transfer Server Storage for VMware Cloud Director on Linux

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 VMware Cloud Director server group.

Each member of the server group mounts this volume at the same mountpoint: `/opt/vmware/vcloud-director/data/transfer`. Space on this volume is consumed in many ways, including:

- 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.

Shared Storage Options

A traditional Linux-based NFS server or other solutions like Microsoft Windows Server, the VMware vSAN File Service NFS feature, and so on, can provide the shared storage. Starting with vSAN 7.0, you can use the vSAN File Service functionality to export NFS shares by using NFS 3.0 and NFS 4.1 protocols. For more information about vSAN File Service, see the *Administering VMware vSAN* guide in the VMware vSphere Product Documentation.

Requirements for Configuring the NFS Server

There are specific requirements for the NFS server configuration, so that VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.

Linux NFS Server Example

If the Linux NFS server has a directory named vCDspace as the transfer space for the VMware Cloud 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 three cells named vCD-Cell1-IP, vCD-Cell2-IP, and vCD-Cell3-IP is the `no_root_squash` method. You must add the following lines to the `/etc/exports` file.

```
/nfs/vCDspace vCD_Cell1_IP_Address(rw,sync,no_subtree_check,no_root_squash)
/nfs/vCDspace vCD_Cell2_IP_Address(rw,sync,no_subtree_check,no_root_squash)
/nfs/vCDspace vCD_Cell3_IP_Address(rw,sync,no_subtree_check,no_root_squash)
```

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.

For each server in the VMware Cloud Director server group, you must have a corresponding entry in the NFS server's `/etc/exports` file so that they can all mount this NFS share. After making changes to the `/etc/exports` file on the NFS server, run `exportfs -a` to re-export all NFS shares.

Considerations When Planning to Upgrade Your VMware Cloud Director Installation to a Later Version

During an upgrade of a VMware Cloud Director server group, you run the installation file for the upgraded version to upgrade all the members of the VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director

If you plan your VMware Cloud 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 VMware Cloud Director installation.

NSX Manager is included in the NSX Data Center for vSphere download. For the most recent information about compatibility between VMware Cloud 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 VMware Cloud Director.

Important This procedure applies only when you are performing a new installation of VMware Cloud Director. If you are upgrading an existing installation of VMware Cloud Director, see Upgrading VMware Cloud Director on Linux.

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 VMware Cloud Director in your planned VMware Cloud Director installation.

4. Configure VXLAN support in the associated NSX Manager instances.

   VMware Cloud 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 VMware Cloud Director

If you plan your VMware Cloud Director installation to use network resources from NSX-T Data Center, you must install and configure NSX-T Data Center.

Important To configure the NSX-T Data Center objects and tools, use the simplified policy UI and the policy APIs that correspond to the simplified UI. For more information, see the overview of NSX-T Manager in the *NSX-T Data Center Administration Guide*.

For the most recent information about compatibility between VMware Cloud Director and other VMware products, see VMware Product Interoperability Matrices.

For information about the network requirements, see Network Configuration Requirements for VMware Cloud Director.

This procedure applies only when you are performing a new installation of VMware Cloud Director. If you are upgrading an existing installation of VMware Cloud Director, see Upgrading VMware Cloud Director on Linux.

Prerequisites

Familiarize yourself with NSX-T Data Center.

Procedure

1 Deploy and configure the NSX-T Manager virtual appliances.

   For more information on NSX-T Manager deployment, see the *NSX-T Data Center Installation Guide*.

2 Create transport zones based on your networking requirements.

   For more information on transport zones creation, see the *NSX-T Data Center Installation Guide*.

   Note

3 Deploy and configure Edge nodes and an Edge cluster.

   For more information on NSX Edge creation, see the *NSX-T Data Center Installation Guide*.

4 Configure the ESXi host transport nodes.

   For more information on configuring a managed host transportation node, see the *NSX-T Data Center Installation Guide*.

5 Create a tier-0 gateway.

   For more information on tier-0 creation, see the *NSX-T Data Center Administration Guide*.

What to do next

After you install VMware Cloud Director, you can:

1 Register the NSX-T Manager instance with your cloud.

   For information about registering an NSX-T Manager instance, see the *VMware Cloud Director Service Provider Admin Portal Guide*.

2 Create a network pool backed by an NSX-T Data Center transport zone.

   For more information on creating a network pool that is backed by an NSX-T Data Center transport zone, see the *VMware Cloud Director Service Provider Admin Portal Guide*.

3 Import the tier-0 gateway as an external network.

   For more information on adding an external network that is backed by an NSX-T Data Center tier-0 logical router, see the *VMware Cloud Director Service Provider Admin Portal Guide*.

Install VMware Cloud Director on Linux

You can create a VMware Cloud Director server group by installing the VMware Cloud 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 VMware Cloud Director installation, see Upgrading VMware Cloud Director on Linux.

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

Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify the server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after the VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Denylist.

Prerequisites

- Verify that the target servers for your server group meet the Chapter 2 VMware Cloud 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 VMware Cloud Director on Linux.
- Verify that you prepared an NFS or other shared storage volume that is accessible to all target servers for your VMware Cloud Director server group. See Preparing the Transfer Server Storage for VMware Cloud Director on Linux.
- Verify that you created a VMware Cloud Director database that is accessible to all servers in the group. See Configure an External PostgreSQL Database for VMware Cloud Director on Linux. Verify that the database service starts when you reboot the database server.
- Verify that all VMware Cloud 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 VMware Cloud Director.
- Verify that all VMware Cloud Director servers and the database server are synchronized to a network time server with the tolerances noted in Network Configuration Requirements for VMware Cloud Director.
- If you plan to import users or groups from an LDAP service, verify that the service is accessible to each VMware Cloud Director server.

- Open firewall ports as shown in Network Security Requirements. Port 443 must be open between VMware Cloud Director and vCenter Server systems.

Procedure

1 Install VMware Cloud Director on the First Member of a Server Group

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

2 SSL Certificate Creation and Management for VMware Cloud Director on Linux

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

3 Configure the Network and Database Connections

After you install VMware Cloud 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.

4 Install VMware Cloud Director on an Additional Member of a Server Group

You can add servers to a VMware Cloud 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.

What to do next

Use the system-setup command of the cell management tool to initialize the server group's database with a system administrator account and related information. See Configure a VMware Cloud Director Installation .

Install VMware Cloud Director on the First Member of a Server Group

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

VMware Cloud 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 VMware Cloud Director.

The VMware Cloud Director installer verifies that the target server meets all platform prerequisites and installs VMware Cloud 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 VMware Cloud 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 VMware Cloud 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.

SSL Certificate Creation and Management for VMware Cloud Director on Linux

VMware Cloud Director uses SSL to secure communications between clients and servers. Each VMware Cloud 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.

Before You Create SSL Certificates for VMware Cloud Director on Linux

When you install VMware Cloud 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 VMware Cloud Director on Linux. The VMware Cloud Director appliance creates self-signed SSL certificates during its first boot.

Procedure

1 Log in to the VMware Cloud 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 VMware Cloud Director on Linux.
- For information on creating self-signed SSL certificates, see Create Self-Signed SSL Certificates for VMware Cloud 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 VMware Cloud Director on Linux.

Create Self-Signed SSL Certificates for VMware Cloud Director on Linux

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

Each VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director cell. See Configure the Network and Database Connections.

Create an CA-Signed SSL Certificate Keystore for VMware Cloud 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 VMware Cloud Director server requires two SSL certificates to secure communications between clients and servers. Each VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 HTTPS and Console Proxy Endpoints.

Procedure

1. Log in directly or by using an SSH client to the OS of the VMware Cloud 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 VMware Cloud 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 PKCS12 -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 PKCS12 -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 PKCS12 keystore.

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

```
keytool -import -storetype PKCS12 -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 PKCS12 -storepass keystore_password -keystore
certificates.ks -alias intermediate -file intermediate_certificate_file
```

c Import the HTTPS service certificate.

```
keytool -import -storetype PKCS12 -storepass keystore_password -keystore
certificates.ks -alias http -file http_certificate_file
```

d Import the console proxy service certificate.

```
keytool -import -storetype PKCS12 -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 PKCS12 keystore, run the command to list the contents of the keystore file.

```
keytool -storetype PKCS12 -storepass keystore_password -keystore certificates.ks -list
```

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

What to do next

- If you have not yet configured your VMware Cloud Director instance, run the `configure` script to import the certificates keystore to VMware Cloud 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 VMware Cloud Director instance, use the `certificates` command of the cell management tool to import the certificates keystore. See Replacing Certificates for the HTTPS and Console Proxy Endpoints.

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

If you have your own private key and CA-signed certificate files, before importing the keystores to your VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 HTTPS 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.p12 -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.p12 -chain
```

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

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

```
keytool -importkeystore -deststorepass keystore_password -destkeystore certificates.ks
-deststoretype PKCS12 -srckeystore http.p12 -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 PKCS12 -srckeystore consoleproxy.p12 -srcstoretype PKCS12 -srcstorepass
keystore_password
```

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

```
keytool -storetype PKCS12 -storepass keystore_password -keystore certificates.ks -list
```

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

What to do next

- If you have not yet configured your VMware Cloud Director instance, run the `configure` script to import the certificates keystore to VMware Cloud 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 VMware Cloud Director instance, use the `certificates` command of the cell management tool to import the certificates keystore. See Replacing Certificates for the HTTPS and Console Proxy Endpoints.

Configure the Network and Database Connections

After you install VMware Cloud 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 VMware Cloud Director server group share database connection and other configuration details. When you run the configuration script on the first member of the VMware Cloud 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 HTTPS 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 Chapter 5 Cell Management Tool Reference.

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 VMware Cloud Director is installed. This value is typically `/opt/vmware/vcloud-director`.

Procedure

1 Log in to the VMware Cloud 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 Cloud Director Setup** wizard after the VMware Cloud Director service starts.

c Offers to start the VMware Cloud Director cell.

3 (Optional) Take a note of the **VMware Cloud Director Setup** wizard URL and enter **y** to start the VMware Cloud 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 4-1. Required Information During an Interactive Network and Database Configuration

Required Information	Description
IP address for the HTTPS 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 HTTPS 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 VMware Cloud Director on Linux.
Private key password for the HTTPS SSL certificate	See Before You Create SSL Certificates for VMware Cloud Director on Linux.
Private key password for the console proxy SSL certificate	See Before You Create SSL Certificates for VMware Cloud Director on Linux.
Enable remote audit logging to a syslog host	Services in each VMware Cloud Director cell log audit messages to the VMware Cloud Director database, where they are preserved for 90 days. To preserve audit messages longer, you can configure VMware Cloud Director services to send audit messages to the `syslog` utility in addition to the VMware Cloud 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.
Host name or IP address of the database server	The server running the database.
Database port	Defaults to 5432.
Database name	Defaults to vcloud.
Database user name	See Configure an External PostgreSQL Database for VMware Cloud Director on Linux.

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

Required Information	Description
Database password	See Configure an External PostgreSQL Database for VMware Cloud Director on Linux.
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 Chapter 5 Cell Management Tool Reference. To join the program, enter **y**. If you prefer not to join the VMware's CEIP program, enter **n**.

Unattended Configuration Reference

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

Table 4-2. Configuration Utility Options and Arguments

Option	Argument	Description
`--help` (`-h`)	None	Displays a summary of configuration options and arguments
`--config-file` (`-c`)	Path to the `global.properties` file	Information that you supply when you run the configuration utility is saved in this file. If you omit this option, the default location is `/opt/vmware/vcloud-director/etc/global.properties`.
`--console-proxy-ip` (`-cons`)	IPv4 address, with optional port number	The system uses this address for the VMware Cloud 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 VMware Cloud Director console proxy service.

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

Option	Argument	Description
`--database-ssl`	`true` or `false`	You can configure the PostgreSQL database to require a well-signed SSL connection from VMware Cloud Director. 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 VMware Cloud Director database host	See Configure an External PostgreSQL Database for VMware Cloud Director on Linux.
`--database-name` (`-dbname`)	The database service name	See Configure an External PostgreSQL Database for VMware Cloud Director on Linux.
`--database-password` (`-dbpassword`)	Password for the database user. It can be null.	See Configure an External PostgreSQL Database for VMware Cloud Director on Linux.
`--database-port` (`-dbport`)	Port number used by the database service on the database host	See Configure an External PostgreSQL Database for VMware Cloud Director on Linux.
`--database-type` (`-dbtype`)	The database type. The supported type is `postgres`.	Optional. The database type will default to `postgres`. See Configure an External PostgreSQL Database for VMware Cloud Director on Linux.
`--database-user` (`-dbuser`)	User name of the database user.	See Configure an External PostgreSQL Database for VMware Cloud Director on Linux.
`--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 Chapter 5 Cell Management Tool Reference.

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

Option	Argument	Description
`--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 VMware Cloud 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 VMware Cloud Director Web interface service
`--primary-port-https`	Integer in the range 0 - 65535	Port number to use for HTTPS (secure) connections to the VMware Cloud 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 VMware Cloud Director cell log audit messages to the VMware Cloud Director database, where they are preserved for 90 days. To preserve audit messages longer, you can configure VMware Cloud Director services to send audit messages to the `syslog` utility in addition to the VMware Cloud 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.
`--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.

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

Option	Argument	Description
`--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 VMware Cloud Director server with two different IP addresses for the HTTPS service and console proxy service.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./configure -ip 10.17.118.159 -cons
10.17.118.158 \
-dbtype postgres -dbhost 10.150.10.78 -dbname postgresql-db-name -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 VMware Cloud Director server with a single IP address with two different ports for the HTTPS 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 postgres -dbhost 10.150.10.78 -dbname postgresql-db-
name \
-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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director on an Additional Member of a Server Group

You can add servers to a VMware Cloud 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 VMware Cloud Director installations on Linux and VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director cell.

9 (Optional) Enter **`y`** to start the VMware Cloud 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 VMware Cloud Director services are running on all servers, you must initialize the VMware Cloud Director database with a license key, system administrator account, and related information. You can initialize the database by using the cell management tool with the `system-setup` subcommand. See Configure a VMware Cloud Director Installation .

After You Install VMware Cloud Director

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

Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify the server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after the VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Denylist.

Customize Public Addresses for VMware Cloud Director on Linux

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

Prerequisites

Verify that you are logged in as a **system administrator**. Only a **system administrator** can customize the public endpoints.

Procedure

1. From the top navigation bar of the Service Provider Admin Portal, select **Administration**.
2. In the left pane, under **Settings**, click **Public Addresses**.
3. To customize the public endpoints, click **Edit**.
4. To customize the VMware Cloud Director URLs, edit the **Web Portal** endpoints.
   a. Enter a custom VMware Cloud Director public URL for HTTP (non-secure) connections.
   b. Enter a custom VMware Cloud Director public URL for HTTPS (secure) connections and click **Upload** to upload the certificates that establish the trust chain for that endpoint.

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

5 (Optional) To customize the Cloud Director REST API and OpenAPI URLs, turn off the **Use Web Portal Settings** toggle.

   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 VMware Cloud Director API at `http://vcloud.example.com/api`, and you can access the VMware Cloud Director OpenAPI at `http://vcloud.example.com/cloudapi`.

   b Enter a custom HTTPS REST API base URL and click **Upload** 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 VMware Cloud Director API at `https://vcloud.example.com/api`, and you can access the VMware Cloud Director 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 VMware Cloud 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 the `PEM` format without a private key.

6 Enter a custom VMware Cloud Director public console proxy address.

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

   Important The VMware Cloud Director appliance uses its `eth0` NIC with custom port 8443 for the console proxy service.

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

   VMware Cloud Director uses the console proxy address when opening a remote console window on a VM.

7 To save your changes, click **Save**.

Install and Configure a Cassandra Database for Storing Historic Metric Data

VMware Cloud 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 VMware Cloud 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 VMware Cloud Director. Retrieval of current metrics does not require optional database software.

Prerequisites

- Verify that VMware Cloud 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 *VMware Cloud 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 VMware Cloud 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 Chapter 5 Cell Management Tool Reference.

2 (Optional) If you are upgrading VMware Cloud 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 VMware Cloud Director cell.

Perform Additional Configurations on the External PostgreSQL Database

After creating your VMware Cloud Director server group, you can configure the external PostgreSQL database to require SSL connections from the VMware Cloud 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 VMware Cloud 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 VMware Cloud Director and the PostgreSQL database.

a If you used a self-signed or private certificate for the external PostgreSQL database, from each VMware Cloud Director cell, run the command to import the database certificate to the VMware Cloud 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 VMware Cloud 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 Chapter 5 Cell Management Tool Reference.

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 VMware Cloud 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.

Install and Configure a RabbitMQ AMQP Broker

If you want to use blocking tasks, notifications, or VMware Cloud Director API extensions, like Container Service Extension (CSE) and VMware Cloud Director App Launchpad, you must install and configure a RabbitMQ AMQP Broker.

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

For VMware Cloud Director, using an MQTT client can be an alternative to the RabbitMQ AMQP Broker when configuring notifications. See Subscribe to Events, Tasks, and Metrics by Using an MQTT Client.

Procedure

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

See the *VMware Cloud 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 VMware Cloud Director cell.

3 During the RabbitMQ installation, make a note of the values that are required for configuring VMware Cloud 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` for non-SSL. The default port for SSL/TLS is `5671`.
   - The communication protocol is TCP.
   - The RabbitMQ virtual host. The default is "`/`".

What to do next

By default, the VMware Cloud 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 VMware Cloud Director cell, typically at `$VCLOUD_HOME/jre/lib/security/cacerts`.

To enable SSL with the VMware Cloud Director AMQP service, see the Configure an AMQP Broker information in the *VMware Cloud Director Service Provider Admin Portal Guide*.

Subscribe to Events, Tasks, and Metrics by Using an MQTT Client

You can use an MQTT client to subscribe to messages about VMware Cloud Director events and tasks.

MQTT is a lightweight, binary, messaging transport protocol. VMware Cloud Director uses MQTT to publish information about events and tasks to which you can subscribe by using an MQTT client. MQTT messages pass through an MQTT broker which can also store messages in case the clients are not online.

Starting with VMware Cloud Director 10.2.2, you can use an MQTT client to subscribe to metrics.

Prerequisites

- Verify that you have an MQTT client that supports WebSocket.
- Verify that you can add headers to a WebSocket-upgraded request.
- If you want to subscribe to metrics, configure the metrics collection and enable metrics publishing. See Configure Metrics Collection and Publishing.

Procedure

1 Log in to VMware Cloud Director by using the OpenAPI endpoint.

2 To establish a WebSocket connection, set the Sec-WebSocket-Protocol property to `mqtt`, set the client to connect to the `/messaging/mqtt` path, add an authorization header, and follow the standard MQTT connect flow.

   You receive the JWT token from the standard login request to VMware Cloud Director. You can leave the user name and password empty.

   ```
   Sec-WebSocket-Protocol: mqtt
   ```

   ```
   Authorization: Bearer {JWT_token}
   ```

3 Once the connection is established successfully, subscribe to topics through the MQTT client.

   ```
   publish/{user_org_id}/{user_id}
   ```

   ```
   publish/debd63a0-6eae-11ea-8c7b-0050561776be/d19fd8ff-6eae-11ea-bb42-0050561776c8
   ```

   Organization administrators can use wildcards to access all organization topics.

   ```
   publish/{user_org_id}/+
   ```

   System administrators can use wildcards to access all topics.

   ```
   publish/#
   ```

4 (Optional) For VMware Cloud Director 10.2.2 or later, subscribe to metrics.

   ```
   metrics/{org_id}/{vApp_id}
   ```

   Only **system administrators** can access the metrics topic.

Auto Scale Groups

Starting with VMware Cloud Director 10.2.2, you can allow tenant users to auto scale applications depending on the current CPU and memory use.

Depending on predefined criteria for the CPU and memory use, tenants can use VMware Cloud Director to automatically scale up or down the number of VMs in a selected scale group. To allow tenants to auto scale applications, you must configure, publish, and grant access to the auto scale solution.

To balance the load of the servers that you configure to run the same application, you can use VMware NSX Advanced Load Balancer (Avi Networks).

Configure and Publish the Auto Scale Plug-in

Before granting access to tenants, you must configure the auto scale groups solution. You can use auto scaling starting from VMware Cloud Director 10.2.2.

1 Log in directly or by using an SSH client to the OS of any of the cells in the cluster as **root**.

2 Enable metric data collection by setting up the metrics collection in a Cassandra database or collect metrics without metrics data persistence.

- Install and Configure a Cassandra Database for Storing Historic Metric Data
- To collect metrics data without data persistence, run the following commands:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.collect.only -v true
```

3 Enable the publishing of metrics.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
statsFeeder.metrics.publishing.enabled -v true
```

4 Create a `metrics.groovy` file in the `/tmp` folder with the following contents.

```
configuration {
    metric("cpu.ready.summation") {
        currentInterval=20
        historicInterval=20
        entity="VM"
        instance=""
        minReportingInterval=300
        aggregator="AVERAGE"
    }
}
```

5 Import the file.

```
$VCLOUD_HOME/bin/cell-management-tool configure-metrics --metrics-config /tmp/
metrics.groovy
```

6 If you previously configured Cassandra, update the Cassandra schema by providing the correct nodes addresses, database authentication details, port and metrics time to live in days.

```
$VCLOUD_HOME/bin/cell-management-tool cassandra -configure -cluster-nodes
nodes_IP_addresses -username cassandra -password cassandra_password -port port_number -ttl
TTL_days -update-schema
```

7 If you run the cell with a CA-signed certificate, to enable auto scaling, run the following command.

```
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --set enabled=true
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --set username=<username>
$VCLOUD_HOME/bin/cell-management-tool configure-autoscale --encrypt --set
password=<password>
```

When running the command from the terminal, escape any special characters using the backslash (\) sign.

8 Restart the cell.

```
service vmware-vcd restart
```

9 Publish the Auto Scale Rights Bundle

Publish the Auto Scale Rights Bundle

If you want tenants to auto scale applications, you must publish the rights bundle to one or more organizations in your system. You can use auto scaling starting from VMware Cloud Director 10.2.2.

Prerequisites

Configure and Publish the Auto Scale Plug-in

Procedure

1 From the top navigation bar, select **Administration**.

2 In the left panel, under **Tenant Access Control**, select **Rights Bundles**.

3 Verify that there are no **Legacy Rights Bundles** for the tenant organizations to which you want to grant access to auto scaling.

4 Select the **vmware:scalegroup Entitlement** bundle, and click **Publish**.

5 To publish the bundle:

a Select **Publish to Tenants**.

b Select the organizations to which you want to publish the role.

- If you want to publish the bundle to all existing and newly created organizations in your system, select **Publish to All Tenants**.
- If you want to publish the bundle to particular organizations in your system, select the organizations individually.

6 Click **Save**.

What to do next

Add the necessary **VMWARE:SCALEGROUP** rights to the tenant roles that you want to use scale groups. See View and Edit a Global Tenant Role in the *VMware Cloud Director Service Provider Admin Portal Guide*.

Upgrading VMware Cloud Director on Linux

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

If your existing VMware Cloud Director server group consists of VMware Cloud Director installations on Linux, you can use the VMware Cloud Director installer for Linux to upgrade your environment.

For VMware Cloud Director installations on Linux, you can either perform an orchestrated upgrade, or manually upgrade VMware Cloud Director. See Perform an Orchestrated Upgrade of a VMware Cloud Director Installation or Manually Upgrade a VMware Cloud 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 VMware Cloud Director 9.5:

- Oracle databases are unsupported. If your existing VMware Cloud Director installation uses an Oracle database, see the Upgrade Paths and Workflows table.
- Activating and deactivating ESXi hosts is unsupported. Before starting the upgrade, you must activate all ESXi hosts. You can place the ESXi hosts in maintenance mode by using the vSphere Client.
- VMware Cloud 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.

Starting with VMware Cloud Director 10.0, Microsoft SQL Server databases are unsupported.

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

- The database software you are currently using for the VMware Cloud Director database. For more information, see the Upgrade and Migration Paths table.
- The VMware vSphere ® release you are currently using.
- The VMware NSX® release that you are currently using.
- Any third-party components that directly interact with VMware Cloud Director.

For information about the compatibility of VMware Cloud 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 your vSphere or NSX components as part of the VMware Cloud Director upgrade, you must upgrade them after the upgrade of VMware Cloud Director. See After You Upgrade VMware Cloud Director.

After you upgrade at least one VMware Cloud Director server, you can upgrade the VMware Cloud Director database. The database stores information about the runtime state of the server, including the state of all VMware Cloud 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 VMware Cloud Director database:

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

The upgrade requires sufficient VMware Cloud 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.`

Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify the server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after the VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Denylist.

Important After upgrading to version 10.1 and later, VMware Cloud Director always verifies certificates for any infrastructure endpoints connected to it. This is due to a change in the way VMware Cloud Director manages SSL certificates. If you do not import your certificates into VMware Cloud Director before the upgrade, the vCenter Server and NSX connections might show failed connection errors due to SSL verification issues. In this case, after upgrading, you have two options:

1. Run the cell management tool `trust-infra-certs` command to import automatically all certificates into the centralized certificate store. See Import Endpoints Certificates from vSphere Resources.
2. In the Service Provider Admin Portal UI, select each vCenter Server and NSX instance, and reenter the credentials while accepting the certificate.

Upgrade Paths and Workflows

Source environment	Target environment VMware Cloud Director 10.2 on Linux with an external PostgreSQL database
VMware Cloud Director 9.7 on Linux with an external Microsoft SQL Server database	1 Migrate the Microsoft SQL Server database to a PostgreSQL database. See Migrate to PostgreSQL database. 2 Upgrade your environment to VMware Cloud Director 10.2 on Linux. See Perform an Orchestrated Upgrade of a VMware Cloud Director Installation or Manually Upgrade a VMware Cloud Director Installation.
VMware Cloud Director 9.7, 10.0, or 10.1 on Linux with an external PostgreSQL database	Upgrade your environment to VMware Cloud Director 10.2 on Linux. See Perform an Orchestrated Upgrade of a VMware Cloud Director Installation or Manually Upgrade a VMware Cloud Director Installation.
VMware Cloud Director appliance 9.7, 10.0, or 10.1 with an embedded PostgreSQL database	Not supported

Perform an Orchestrated Upgrade of a VMware Cloud Director Installation

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

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

VMware Cloud 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 VMware Cloud Director.

When you run the VMware Cloud 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 VMware Cloud Director database, the vSphere components, and the NSX components are compatible with the new version of VMware Cloud Director.

  Important If your existing VMware Cloud Director installation uses an Oracle database or a Microsoft SQL Server database, verify that you migrated to a PostgreSQL database before the upgrade. For the possible upgrade paths, see Upgrading VMware Cloud Director on Linux.

- 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 VMware Cloud 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 VMware Cloud Director installer for use as an identity with which VMware Cloud 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 for VMware Cloud Director on Linux.
- If your VMware Cloud 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 VMware Cloud 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 VMware Cloud Director and prompts you to confirm the upgrade.

   If the installer detects a version of VMware Cloud 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 VMware Cloud Director RPM package.

3 Upgrades VMware Cloud Director software on the current cell.

4 Upgrades the VMware Cloud Director database.

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

6 Restarts VMware Cloud Director services on the current cell.

What to do next

Start the VMware Cloud 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 VMware Cloud Director Installation

You can upgrade a single cell by running the VMware Cloud 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 VMware Cloud Director installer for Linux to upgrade a VMware Cloud Director server group that consists of VMware Cloud Director installations on a supported Linux OS. If your VMware Cloud Director server group consists of VMware Cloud Director 9.5 appliances deployments, you use the VMware Cloud Director installer for Linux to upgrade your existing environment only as part of the migration workflow. See Upgrading and Migrating the VMware Cloud Director Appliance.

For a multi-cell VMware Cloud Director installation, instead of manually upgrading each cell and the database in a sequence, you can perform an orchestrated upgrade of the VMware Cloud Director installation. See Perform an Orchestrated Upgrade of a VMware Cloud Director Installation.

Prerequisites

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

  Important If your existing VMware Cloud Director installation uses an Oracle database or a Microsoft SQL Server database, verify that you migrated to a PostgreSQL database before the upgrade. For the possible upgrade paths, see Upgrading VMware Cloud Director on Linux.

- Verify that you have superuser credentials for the servers in your VMware Cloud 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 VMware Cloud Director software to which you are upgrading.

- Verify that you all ESXi hosts are activated. Deactivated ESXi hosts are unsupported.

Procedure

1 Upgrade a VMware Cloud Director Cell

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

2 Upgrade the VMware Cloud Director Database

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

What to do next

- After you upgraded all VMware Cloud Director servers in the server group and the database, you can start the VMware Cloud Director services on all cells.
- Upgrade Each NSX Manager That Is Associated with an Attached vCenter Server System
- After upgrading each NSX Manager, you can upgrade the vCenter Server systems, hosts, and NSX edges. See Upgrade vCenter Server Systems, ESXi Hosts, and NSX Edges.

Upgrade a VMware Cloud Director Cell

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

VMware Cloud 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 VMware Cloud Director.

For a multi-cell VMware Cloud Director installation, you must run the VMware Cloud Director installer on each member of the VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud 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 VMware Cloud Director RPM package.

   c After all active VMware Cloud Director jobs on the cell finish, stops VMware Cloud Director services on the server and upgrades the installed VMware Cloud 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 VMware Cloud 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 VMware Cloud Director database.

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

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

Upgrade the VMware Cloud Director Database

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

Information about all running and recently completed tasks is stored in the VMware Cloud 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 VMware Cloud 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, VMware Cloud 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 VMware Cloud Director cells in the server group are stopped. The upgraded cells are stopped during the upgrade process. If there are VMware Cloud 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 Chapter 5 Cell Management Tool Reference.
- Review the Database Upgrade Utility Reference topic.

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 VMware Cloud 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 VMware Cloud Director servers.

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

The location of the `upgrade` utility is `/opt/vmware/vcloud-director/bin/`.

Table 4-3. Database Upgrade Utility Options and Arguments

Option	Argument	Description
`--backup-completed`	None	Specifies that you have completed a backup of the VMware Cloud Director. When you include this option, the upgrade utility does not prompt you to back up the database.
`--ceip-user`	The user name for the CEIP service account.	If a user with this user name already exists in the System organization, the upgrade fails. 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 can use the cell management tool to join or leave VMware's CEIP for this product at any time. See Chapter 5 Cell Management Tool Reference.
`--installer-path`	Full pathname to the VMware Cloud Director installation file. The installation file and the directory in which it is stored must be readable by the user vcloud.vcloud.	Requires `--private-key-path` option.

Table 4-3. 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 restarted, this cell is shut down and upgraded. Requires `--private-key-path` option.
`--multisite-user`	The user name for the Multi-Site system account.	This account is used by the VMware Cloud Director Multi-Site feature. If a user with this user name already exists in the System organization, the upgrade fails. 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 restarted after the database has been upgraded. See Perform an Orchestrated Upgrade of a VMware Cloud 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 VMware Cloud Director installer for use as an identity with which VMware Cloud Director processes run. The `vcloud` user has no password.

After You Upgrade VMware Cloud Director

After you upgrade all VMware Cloud 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 VMware Cloud Director installation.

Important VMware Cloud 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.

Starting with version 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers, and to verify the server identity as part of an SSL handshake. To protect VMware Cloud Director network connections, configure a deny list of internal hosts that are unreachable to tenants who are using the VMware Cloud Director API for connection testing. Configure the deny list after the VMware Cloud Director installation or upgrade and before granting tenants access to VMware Cloud Director. See Configure a Test Connection Denylist.

Important After upgrading to version 10.1 and later, VMware Cloud Director always verifies certificates for any infrastructure endpoints connected to it. This is due to a change in the way VMware Cloud Director manages SSL certificates. If you do not import your certificates into VMware Cloud Director before the upgrade, the vCenter Server and NSX connections might show failed connection errors due to SSL verification issues. In this case, after upgrading, you have two options:

1. Run the cell management tool `trust-infra-certs` command to import automatically all certificates into the centralized certificate store. See Import Endpoints Certificates from vSphere Resources.
2. In the Service Provider Admin Portal UI, select each vCenter Server and NSX instance, and reenter the credentials while accepting the certificate.

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

Before you upgrade a vCenter Server and ESXi hosts registered to VMware Cloud 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 VMware Cloud Director, whether or not any VMware Cloud 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 VMware Cloud 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 VMware Cloud Director and NSX Manager, you must upgrade the vCenter Server systems and ESXi hosts that are registered to VMware Cloud 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. From the top navigation bar of the VMware Cloud Director Service Provider Admin Portal, under **Resources**, select **vSphere Resources**.
   b. In the left panel, click **vCenter Server Instances**.
   c. Select the radio button next to the vCenter Server instance you want to deactivate and click **Disable**.
   d. Click **OK**.
2. Upgrade the vCenter Server system.

   For information, see *vCenter Server Upgrade*.
3. Verify all VMware Cloud Director public URLs and certificate chains.
   a. From the top navigation bar, select **Administration**.
   b. In the left panel, under **Settings**, click **Public Addresses**.
   c. Verify all public addresses.

4 Refresh the vCenter Server registration with VMware Cloud Director.

   a From the top navigation bar of the VMware Cloud Director Service Provider Admin Portal, under **Resources**, select **vSphere Resources**.

   b In the left panel, click **vCenter Server Instances**.

   c Select the radio button next to the target vCenter Server and click **Reconnect**.

   d Click **OK**.

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 VMware Cloud 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 VMware Cloud Director to upgrade an NSX Edge Gateway, you must operate on the VMware Cloud Director network object that the Edge supports:
     - An appropriate upgrade of an Edge Gateway occurs automatically when you use either the VMware Cloud Director or VMware Cloud Director API to reset a network that the Edge Gateway serves.
     - Redeploying an Edge Gateway upgrades the associated NSX Edge appliance.

       Note Redeploying is supported only for NSX Data Center for vSphere Edge Gateways.

- Resetting a vApp network from within the context of the vApp upgrades the NSX Edge appliance associated with that network. To reset a vApp network from within the context of a vApp, navigate to the **Networks** tab for the vApp, display its networking details, click the radio button next to the name of the vApp network, and click **Reset**.

For more information on how to redeploy Edge Gateways and reset vApp networks, see the *VMware Cloud Director API Programming Guide*.

What to do next

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

Cell Management Tool Reference 5

The cell management tool is a command-line utility that you can use to manage a VMware Cloud Director cell or database. Superuser or system administrator credentials are required for most operations.

The cell management tool is installed in `/opt/vmware/vcloud-director/bin/`. You can use it to run a single command or run it as an interactive shell.

Listing Available Commands

To list the available cell management tool commands, use the following command line.

```
./cell-management-tool -h
```

Using Shell Mode

You can run the cell management tool as an interactive shell by invoking it with no arguments, as shown here.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool
Cell Management Tool v8.14.0.4146350
Type "help" for available subcommands.
cmt>
```

While in shell mode, you can type any cell management tool command at the `cmt>` prompt, as shown in this example.

```
cmt>cell -h
usage: cell [options]
               -a,--application-states     display the state of each application
                                           on the cell [DEPRECATED - use the
                                           cell-application command instead]
               -h,--help                   print this message
               -i,--pid <arg>              the process id of the cell [REQUIRED
                                           if username is not specified]
               -m,--maintenance <arg>      gracefully enter maintenance mode on
                                           the cell
               -p,--password <arg>         administrator password [OPTIONAL]
               -q,--quiesce <arg>          quiesce activity on the cell
               -s,--shutdown               gracefully shutdown the cell
```

```
                -t,--status                 display activity on the cell
                -tt,--status-verbose        display a verbose description of
                                            activity on the cell
                -u,--username <arg>         administrator username [REQUIRED if
                                            pid is not specified]
Note: You will be prompted for administrator password if not entered in command
line.
cmt>
```

The command returns to the `cmt>` prompt when it finishes running. To exit the shell mode, type **`exit`** at the `cmt>` prompt.

Example: Cell Management Tool Usage Help

This example runs a single, non-interactive command that lists available shell management tool commands.

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

usage: cell-management-tool
-h,--help   print this message

Available commands:
cell - Manipulates the Cell and core components
certificates - Reconfigures the SSL certificates for the cell
.
.
.

For command specific help:
 cell-management-tool <commandName> -h
```

- Configure a VMware Cloud Director Installation

  Use the `system-setup` command of the cell management tool to initialize the server group's database with a system administrator account and related information.

- Deactivate the Service Provider Access to the Legacy API Endpoint

  Starting with VMware Cloud Director 10.0, you can use separate VMware Cloud Director OpenAPI login endpoints for the service provider and tenant access to VMware Cloud Director.

- Managing a Cell

  With the `cell` subcommand of the cell management tool, you can suspend the task scheduler so that new tasks cannot be started, view the status of active tasks, control cell maintenance mode, or shut down the cell gracefully.

- Managing Cell Applications

  Use the `cell-application` command of the cell management tool to control the set of applications that the cell runs on startup.

- Updating the Database Connection Properties

  You can update the connection properties for the VMware Cloud Director database by using the `reconfigure-database` subcommand of the cell management tool.

- Detecting and Repairing Corrupted Scheduler Data

  VMware Cloud Director uses the Quartz job scheduler to co-ordinate asynchronous operations (jobs) running on the system. If the Quartz scheduler database becomes corrupted, you might not be able to quiesce the system successfully. Use the `fix-scheduler-data` command of the cell management tool to scan the database for corrupt scheduler data and repair that data as needed.

- Generating Self-Signed Certificates for the HTTPS and Console Proxy Endpoints

  Use the `generate-certs` command of the cell management tool to generate self-signed SSL certificates for the HTTPS and Console Proxy endpoints.

- Replacing Certificates for the HTTPS and Console Proxy Endpoints

  Use the `certificates` command of the cell management tool to replace SSL certificates for the HTTPS and Console Proxy endpoints.

- Importing SSL Certificates from External Services

  Use the `import-trusted-certificates` command of the cell management tool to import certificates for use in establishing secure connections to external services like AMQP and the VMware Cloud Director database.

- Import Endpoints Certificates from vSphere Resources

  After upgrade, use the `trust-infra-certs` command of the cell management tool to collect and import certificates from the vSphere resources in your environment to the VMware Cloud Director database.

- Configure a Test Connection Denylist

  After installation or upgrade, use the `manage-test-connection-blacklist` command of the cell management tool to block access to internal hosts before providing tenants with access to the VMware Cloud Director network.

- View the FIPS Status of All Active Cells

  Starting with VMware Cloud Director 10.2.2, to verify the FIPS status of all active VMware Cloud Director cells, you can use the `fips-status` command. The command does not show the FIPS status of the VMware Cloud Director appliance.

- Managing the List of Allowed SSL Ciphers

  Use the `ciphers` command of the cell management tool to configure the set of cipher suites that the cell offers to use during the SSL handshake process.

- Manage the List of Allowed SSL Protocols

  To configure the set of SSL protocols that the cell offers to use during the SSL handshake process, use the `ssl-protocols` command of the cell management tool.

- Configure Metrics Collection and Publishing

  You can use the `configure-metrics` command of the cell management tool to configure the set of metrics to collect.

- Configuring a Cassandra Metrics Database

  Use the `cassandra` command of the cell management tool to connect the cell to an optional metrics database.

- Recovering the System Administrator Password

  If you know the VMware Cloud Director database username and password, you can use the `recover-password` command of the cell management tool to recover the VMware Cloud Director system administrator password.

- Update the Failure Status of a Task

  Use the `fail-tasks` command of the cell management tool to update the completion status associated with tasks that were running when the cell was deliberately shut down. You cannot use the `fail-tasks` command unless all cells have been shut down.

- Configure Audit Message Handling

  Use the `configure-audit-syslog` command of the cell management tool to configure the way the system logs audit messages.

- Configuring Email Templates

  To manage the templates that the system uses when creating email alerts, you can use the `manage-email` command of the cell management tool.

- Finding Orphaned VMs

  Use the `find-orphan-vms` command of the cell management tool to find references to virtual machines that are present in the vCenter database but not in the VMware Cloud Director database.

- Join or Leave the VMware Customer Experience Improvement Program

  To join or leave the VMware Customer Experience Improvement Program (CEIP), you can use the `configure-ceip` subcommand of the cell management tool.

- Updating Application Configuration Settings

  With the `manage-config` subcommand of the cell management tool, you can update different application configuration settings such as catalog throttling activities.

- Configuring Catalog Synchronization Throttling

  When you have many catalog items published to or subscribed from other organizations, to avoid overloading the system during catalog synchronizations, you can configure catalog synchronization throttling. You can use the `manage-config` subcommand of the cell management tool to configure catalog synchronization throttling by limiting the number of library items that can be synced at the same time.

- Troubleshoot Failed Access to the VMware Cloud Director User Interface

  To view and update the valid IP addresses and DNS entries for the VMware Cloud Director cells in your VMware Cloud Director environment, you can use the `manage-config` subcommand of the cell management tool.

- Debugging vCenter VM Discovery

  By using the `debug-auto-import` subcommand of the cell management tool, you can investigate the reason for which the mechanism for discovering vApps skips one or more vCenter VMs.

- Regenerating MAC Addresses for Multisite Stretched Networks

  If you associate two VMware Cloud Director sites that are configured with the same installation ID, you might encounter MAC address conflicts in stretched networks across these sites. To avoid such conflicts, you must regenerate the MAC addresses in one of the sites based on a custom seed that is different from the installation ID.

- Update the Database IP Addresses on VMware Cloud Director Cells

  To update the IP addresses of the VMware Cloud Director cells in a database high availability cluster, you can use the cell management tool.

Configure a VMware Cloud Director Installation

Use the `system-setup` command of the cell management tool to initialize the server group's database with a system administrator account and related information.

After you configure all servers in the VMware Cloud Director server group and connect them to the database, you can create the initial system administrator account and initialize the VMware Cloud Director database with related information with a command line of the following form:

```
cell-management-tool system-setup  options
```

You cannot run this command on a system that has already been set up. All options except `--unattended` and `--password` must be specified.

Table 5-1. Cell Management Tool Options and Arguments, `system-setup` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--email`	The email address for the system administrator you are creating.	The system administrator's email address is stored in the VMware Cloud Director database.
`--full-name`	The full name of the system administrator you are creating.	The system administrator's full name is stored in the VMware Cloud Director database.

Table 5-1. Cell Management Tool Options and Arguments, `system-setup` Subcommand (continued)

Option	Argument	Description
`--installation-id`	An integer in the range from 1 through 63	The installation ID for this installation of VMware Cloud Director. The system uses the installation ID when generating MAC addresses for virtual NICs. **Note** If you plan to create stretched networks across VMware Cloud Director installations in a multisite deployment, consider setting a unique installation ID for each VMware Cloud Director installation.
`--password`	The password for the system administrator you are creating. Required when you use the `--unattended` option. If you do not use the `--unattended` option, the command prompts you for this password if you do not supply it on the command line.	The system administrator supplies this password when authenticating to VMware Cloud Director.
`--serial-number`	The serial number (license key) for this installation.	Optional. Must be a valid VMware Cloud Director serial number.
`--system-name`	The name to use a name for the VMware Cloud Director vCenter Server folder.	This VMware Cloud Director installation is represented by a folder with this name in each vCenter Server with which it registers.
`--unattended`	None	Optional. The command does not prompt for further input when invoked with this option.
`--user`	The user name of the system administrator you are creating.	The system administrator supplies this user name when authenticating to VMware Cloud Director.

Example: Specify VMware Cloud Director System Settings

A command like this one specifies all system settings for a new VMware Cloud Director installation. Because `--unattended` and `--password` are not specified, the command prompts you to supply and confirm the password to create for the system administrator.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool system-setup \
--user admin --full-name "VCD System Administrator" --email vcd-admin@example.com --system-
name VCD --installation-id 2
Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:

Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
Are you sure you want to use these parameters? [Y/n]:y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.
```

Deactivate the Service Provider Access to the Legacy API Endpoint

Starting with VMware Cloud Director 10.0, you can use separate VMware Cloud Director OpenAPI login endpoints for the service provider and tenant access to VMware Cloud Director.

You can use two new OpenAPI endpoints to increase the security by restricting the access to VMware Cloud Director.

- `/cloudapi/1.0.0/sessions/provider` - OpenAPI endpoint for the service provider login. Tenants cannot access VMware Cloud Director by using this endpoint.
- `/cloudapi/1.0.0/sessions/` - OpenAPI endpoint for the tenant login. Service providers cannot access VMware Cloud Director by using this endpoint.

By default, provider administrators and organization users can access VMware Cloud Director by logging into the `/api/sessions` API endpoint.

By using the `manage-config` subcommand of the cell management tool, you can deactivate the service provider access to the `/api/sessions` API endpoint and, as a result, limit the provider login to the new `/cloudapi/1.0.0/sessions/provider` OpenAPI endpoint that is accessible only to service providers.

Note When you deactivate the service provider access to the `/api/sessions` API endpoint, service provider requests that supply only a SAML token in the authorization header will fail for all legacy API endpoints.

Procedure

1 Log in or SSH as **root** to the OS of any of the VMware Cloud Director cells.

2 To block the provider access to the `/api/sessions` API endpoint, use the cell management tool and run the following command:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v true
```

Results

The `/api/sessions` API endpoint is no longer accessible to service providers. Service providers can use the new OpenAPI endpoint `/cloudapi/1.0.0/sessions/provider` to access VMware Cloud Director. Tenants can access VMware Cloud Director by using both the `/api/sessions` API endpoint and the new `/cloudapi/1.0.0/sessions/` OpenAPI endpoint.

What to do next

To enable the provider access to the `/api/sessions` API endpoint, run the following command:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v false
```

Managing a Cell

With the `cell` subcommand of the cell management tool, you can suspend the task scheduler so that new tasks cannot be started, view the status of active tasks, control cell maintenance mode, or shut down the cell gracefully.

To manage a cell, use a command line with the following form:

```
cell-management-tool cell -u sysadmin-username -p sysadmin-password option
```

where *sysadmin-username* and *sysadmin-password* are the user name and password of the **system administrator**.

Note For security reasons, you can omit the password. In this case, the command prompts you to enter the password without displaying it on the screen.

As an alternative to providing the **system administrator** credentials, you can use the `--pid` option and provide the process ID of the cell process. To find the process ID of the cell, use a command like this one:

```
cat /var/run/vmware-vcd-cell.pid
```

Table 5-2. Cell Management Tool Options and Arguments, `cell` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available commands in this category.
`--pid` (`-i`)	Process ID of the cell process	You can use this option instead of `-username`.
`--maintenance` (`-m`)	`true` or `false`	Sets the cell in maintenance mode. The argument `true` quiesces activity on the cell and puts the cell in maintenance mode. The argument `false` releases the cell from maintenance mode.
`--password` (`-p`)	VMware Cloud Director **system administrator** password	Optional if the `-username` option is used. If you omit this option, the command prompts you to enter the password without displaying it on the screen.
`--quiesce` (`-q`)	`true` or `false`	Quiesces activity on the cell. The argument `true` suspends the scheduler. The argument `false` restarts the scheduler.
`--shutdown` (`-s`)	None	Gracefully shuts down VMware Cloud Director services on the server.
`--status` (`-t`)	None	Displays information about the number of tasks running on the cell and the status of the cell.
`--status-verbose` (`-tt`)	None	Displays verbose information about the tasks running on the cell and the status of the cell.
`--username` (`-u`)	VMware Cloud Director **system administrator** user name.	You can use this option instead of `-pid`.

Managing Cell Applications

Use the `cell-application` command of the cell management tool to control the set of applications that the cell runs on startup.

A VMware Cloud Director runs a number of applications that provide services that VMware Cloud Director clients require. The cell starts a subset of these applications by default. All members of that subset are typically required to support a VMware Cloud Director installation.

To view or change the list of applications that run when the cell starts, use a command line with the following form:

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell-application command
```

sysadmin-username

Username of a VMware Cloud Director system administrator.

sysadmin-password

Password of the VMware Cloud Director system administrator. You must quote the password if it contains special characters.

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

As an alternative to providing system administrator credentials, you can use the `--pid` option and provide the process ID of the cell process. To find the process ID of the cell, use a command like this one:

```
cat /var/run/vmware-vcd-cell.pid
```

command

`cell-application` subcommand.

Table 5-3. Cell Management Tool Options and Arguments, `cell-application` Subcommand

Command	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--application-states`	None	List the cell applications and their current states.
`--disable`	Application ID	Prevent this cell application from running at cell startup.
`--enable`	Application ID	Enable this cell application to run at cell startup.
`--pid` (-i)	Process ID of the cell process	You can use this option instead of `-u` or `-u` and `-p`.
`--list`	None	List all cell applications and show whether they are enabled to run at cell startup.
`--password` (-p)	VMware Cloud Director administrator password	Optional. The command will prompt for the password if you do not supply it on the command line.

Table 5-3. Cell Management Tool Options and Arguments, `cell-application` Subcommand (continued)

Command	Argument	Description
`--set`	Semicolon-separated list of application IDs.	Specify the set of cell applications that run at cell startup. This command overwrites the existing set of cell applications that start at cell startup. Use `--enable` or `--disable` to change the startup state of a single application.
`--username` (-u)	VMware Cloud Director administrator user name.	Required if not specifying `--pid`

Example: Listing Cell Applications and Their Startup States

The following `cell-management-tool` command line requires system administrator credentials and returns the list of cell applications and their startup states.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell-application --list
Please enter the administrator password:

 name                    id              enabled
description

 Networking              com.vmware.vc... true     Exposes NSX api endpoints directly from
vCD.
 Console Proxy           com.vmware.vc... true     Proxies VM console data
connection...
 Cloud Proxy             com.vmware.vc... true     Proxies TCP connections from a tenant
site.
 Compute Service Broker  com.vmware.vc... true     Allows registering with a service
control...
 Maintenance Application com.vmware.vc... false    Indicates to users the cell is
undergo ...
 Core Cell Application   com.vmware.vc... true     Main cell application, Flex UI and REST
API.
```

Updating the Database Connection Properties

You can update the connection properties for the VMware Cloud Director database by using the `reconfigure-database` subcommand of the cell management tool.

During the VMware Cloud Director installation or VMware Cloud Director appliance deployment process, you configure the database type and database connections properties. See Install VMware Cloud Director on Linux and Deployment and Initial Configuration of the VMware Cloud Director Appliance.

After configuring the VMware Cloud Director database, you can update the database connections by using the `reconfigure-database` subcommand. You can move the existing VMware Cloud Director database to a new host, change the database user name and password, or enable an SSL connection for a PostgreSQL database.

```
cell-management-tool reconfigure-database  options
```

Important The changes you make by running the `reconfigure-database` command are written to the global configuration file `global.properties` and the response file `responses.properties` of the cell. Before you run the command, verify that the response file is present at `/opt/vmware/vcloud-director/etc/responses.properties` and writable. For information about protecting and reusing the response file, see Install VMware Cloud Director on Linux.

If you do not use the `--pid` option, you must restart the cell to apply the changes.

Table 5-4. Cell Management Tool Options and Arguments, `reconfigure-database` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available options in this category.
`--database-host` (`-dbhost`)	IP address or fully qualified domain name of the VMware Cloud Director database host	Updates the value of the `database.jdbcUrl` property. **Important** The command validates only the value format.
`--database-instance` (`-dbinstance`)	SQL Server database instance.	Optional. Used if the database type is `sqlserver`. **Important** If you include this option, you must provide the same value that you specified when you originally configured the database.
`--database-name` (`-dbname`)	The database service name.	Updates the value of the `database.jdbcUrl` property.
`--database-password` (`-dbpassword`)	Password for the database user.	Updates the value of the `database.password` property. The password you supply is encrypted before it is stored as a property value.
`--database-port` (`-dbport`)	Port number used by the database service on the database host.	Updates the value for the `database.jdbcUrl` property. **Important** The command validates only the value format.

Table 5-4. Cell Management Tool Options and Arguments, `reconfigure-database` Subcommand (continued)

Option	Argument	Description
`--database-type` (`-dbtype`)	The database type. One of: ■ `sqlserver` ■ `postgres`	Updates the value of the `database.jdbcUrl` property.
`--database-user` (`-dbuser`)	User name of the database user.	Updates the value of the `database.user` property.
`--database-ssl`	`true` or `false`	Used if the database type is `postgres`. Configures the PostgreSQL database to require an SSL connection from VMware Cloud Director.
`--pid` (`-i`)	The process id of the cell.	Optional. Runs a hot reconfiguration on a running VMware Cloud Director cell. Does not require a restart of the cell. If used with the `--private-key-path`, you can run the command on local and remote cells immediately.
`--private-key-path`	Pathname to the private key of the cell.	Optional. All cells in the server group gracefully shut down, update their database properties, and restart. **Important** All cells must permit SSH connections from the superuser without a password.
`--remote-sudo-user`	A user name with sudo rights.	Used with the `--private-key-path` option when the remote user different from **root**. For the appliance, you can use this option for the **postgres** user, for example **`--remote-sudo-user=postgres`**.

When you use options `--database-host` and `--database-port`, the command validates the format of the arguments but does not test the combination of host and port for network accessibility or the presence of a running database of the specified type.

If you use the `--private-key-path` option, all cells must be configured to permit SSH connections from the superuser without a password. To perform a verification, for example, 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 VMware Cloud Director installer for use as an identity with which VMware Cloud Director processes run. The `vcloud` user has no password.

Example: Change the VMware Cloud Director Database User Name and Password

To change the VMware Cloud Director database user name and password, leaving all other connection properties as they were originally configured, you can run the following command:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \
-dbuser vcd-dba -dbpassword P@55w0rd
```

Example: Update the VMware Cloud Director Database IP Address by Hot Reconfiguration on All Cells

If you are a non-root user with sudo rights, to change the IP address of the VMware Cloud Director database on all cells immediately, you can run the following command:

```
[sudo@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \
--dbhost db_ip_address -i $(service vmware-vcd pid cell) --private-key-path=path_to_private-key \
--remote-sudo-user=non-root-user
```

Detecting and Repairing Corrupted Scheduler Data

VMware Cloud Director uses the Quartz job scheduler to co-ordinate asynchronous operations (jobs) running on the system. If the Quartz scheduler database becomes corrupted, you might not be able to quiesce the system successfully. Use the `fix-scheduler-data` command of the cell management tool to scan the database for corrupt scheduler data and repair that data as needed.

To scan database for corrupt scheduler data, use a command line with the following form:

```
cell-management-tool fix-scheduler-data options
```

Table 5-5. Cell Management Tool Options and Arguments, `fix-scheduler-data` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--dbuser`	The user name of the VMware Cloud Director database user.	Must be supplied on the command line.
`--dbpassword`	The password of the VMware Cloud Director database user.	Prompted for if not supplied.

Generating Self-Signed Certificates for the HTTPS and Console Proxy Endpoints

Use the `generate-certs` command of the cell management tool to generate self-signed SSL certificates for the HTTPS and Console Proxy endpoints.

Each VMware Cloud Director server group must support two SSL endpoints: one for the HTTPS service and another for the console proxy service. The HTTPS service endpoint supports the VMware Cloud Director Service Provider Admin Portal, the VMware Cloud Director Tenant Portal, and the VMware Cloud Director API. The remote console proxy endpoint supports VMRC connections to vApps and VMs.

The `generate-certs` command of the cell management tool automates the Create Self-Signed SSL Certificates for VMware Cloud Director on Linux procedure.

To generate new self-signed SSL certificates and add them to a new or existing keystore, use a command line with the following form:

```
cell-management-tool generate-certs options
```

Table 5-6. Cell Management Tool Options and Arguments, `generate-certs` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--expiration` (-x)	*days-until-expiration*	Number of days until the certificates expire. Defaults to 365

Table 5-6. Cell Management Tool Options and Arguments, `generate-certs` Subcommand (continued)

Option	Argument	Description
`--issuer` (-i)	*name=value* [, *name=value*, ...]	X.509 distinguished name of the certificate issuer. Defaults to `CN=FQDN`. where *FQDN* is the fully qualified domain name of the cell or its IP address if no fully qualified domain name is available. If you specify multiple attribute and value pairs, separate them with commas and enclose the entire argument in quotation marks.
`--httpcert` (-j)	None	Generate a certificate for the HTTPS endpoint.
`--type` (-t)	*keystore-type*	Format of the keystore. The default is `PKCS12`. You can also create a `JCEKS` keystore.
`--key-size` (-s)	*key-size*	Size of key pair expressed as an integer number of bits. Defaults to 2048. Key sizes smaller than 1024 are no longer supported per NIST Special Publication 800-131A.
`--keystore-pwd` (-w)	*keystore-password*	Password for the keystore on this host.
`--out` (-o)	*keystore-pathname*	Full pathname to the keystore on this host.
`--consoleproxycert` (-p)	None	Generate a certificate for the console proxy endpoint.

Note To maintain compatibility with previous releases of this subcommand, omitting both `-j` and `-p` has the same result as supplying both `-j` and `-p`.

Example: Creating Self-Signed Certificates

Both of these examples assume a keystore at `/tmp/cell.ks` that has the password `kspw`. This keystore is created if it does not already exist.

This example creates the new certificates using the defaults. The issuer name is set to `CN=Unknown`. The certificate uses the default 2048-bit key length and expires one year after creation.

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

This example creates a new certificate for the HTTPS endpoint only. It also specifies custom values for key size and issuer name. The issuer name is set to `CN=Test, L=London, C=GB`. The new certificate for the HTTPS connection has a 4096-bit key and expires 90 days after creation. The existing certificate for the console proxy endpoint is unaffected.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -j
-o /tmp/cell.ks -w kspw
 -i "CN=Test, L=London, C=GB" -s 4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

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

Replacing Certificates for the HTTPS and Console Proxy Endpoints

Use the `certificates` command of the cell management tool to replace SSL certificates for the HTTPS and Console Proxy endpoints.

The `certificates` command of the cell management tool automates the process of replacing existing certificates with new ones stored in a PKCS12 or a JCEKS formatted keystore. Use the `certificates` command to replace self-signed certificates with signed ones or replace expiring certificates with new ones. To create a keystore containing signed certificates, see Create Self-Signed SSL Certificates for VMware Cloud Director on Linux.

To replace SSL certificates for one or both endpoints use a command with the following form:

```
cell-management-tool certificates options
```

Table 5-7. Cell Management Tool Options and Arguments, `certificates` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--config` (-c)	full pathname to the cell's `global.properties` file	Defaults to `$VCLOUD_HOME/etc/global.properties`.
`--httpks` (-j)	None	Replace the keystore file named `certificates` used by the http endpoint.
`--consoleproxyks` (-p)	None	Replace the keystore file named `proxycertificates` used by the console proxy endpoint.
`--responses` (-r)	full pathname to the cell's `responses.properties` file	Defaults to `$VCLOUD_HOME/etc/responses.properties`.

Table 5-7. Cell Management Tool Options and Arguments, `certificates` Subcommand (continued)

Option	Argument	Description
`--keystore` (-k)	*keystore-pathname*	Full pathname to a PKCS12 or a JCEKS formatted keystore containing the signed certificates. Deprecated `-s` short form replaced by `-k`.
`--keystore-password` (-w)	*keystore-password*	Password for the PKCS12 or JCEKS formatted keystore referenced by the `--keystore` option. Replaces deprecated `-kspassword` and `--keystorepwd` options.

Example: Replacing Certificates

You can omit the `--config` and `--responses` options unless those files were moved from their default locations. In this example, a keystore at `/tmp/my-new-certs.ks` has the password `kspw`. This example replaces the cell's existing http endpoint certificate with the one found in `/tmp/my-new-certs.ks`

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool certificates -j -k /tmp/
my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

Note You must restart the cell after you replace the certificates.

Importing SSL Certificates from External Services

Use the `import-trusted-certificates` command of the cell management tool to import certificates for use in establishing secure connections to external services like AMQP and the VMware Cloud Director database.

Before it can make a secure connection to an external service, VMware Cloud Director must establish a valid chain of trust for that service by importing the service's certificates into its own truststore. To import trusted certificates to the cell's truststore, use a command with the following form:

```
cell-management-tool import-trusted-certificates options
```

Table 5-8. Cell Management Tool Options and Arguments, `import-trusted-certificates` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--destination`	path name	Full path name to the destination truststore. Defaults to `/opt/vmware/vcloud-director/etc/certificates` if not provided on the command line.
`--destination-password`	string	Password for the destination truststore. Defaults to the value of `vcloud.ssl.truststore.password` if not provided on the command line.
`--destination-type`	keystore type	Keystore type of the destination truststore. Can be JKS or JCEKS. Defaults to JCEKS.
`--force`	None	Overwrites the existing certificates in the destination truststore.
`--source`	path name	Full path name to source PEM file.

Example: Importing Trusted Certificates

This example imports the certificates from `/tmp/demo.pem` to the VMware Cloud Director local keystore at `/opt/vmware/vcloud-director/etc/certificates`. VMware Cloud Director stores the keystore password in an encrypted format which the `import-trusted-certificates` command decrypts.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool import-trusted-certificates --source /tmp/demo.pem
```

Import Endpoints Certificates from vSphere Resources

After upgrade, use the `trust-infra-certs` command of the cell management tool to collect and import certificates from the vSphere resources in your environment to the VMware Cloud Director database.

The `trust-infra-certs` command of the cell management tool automatically gathers the SSL certificates from the vSphere resources in your environment and imports them to the VMware Cloud Director database.

Prerequisites

Verify that the vCenter Server and NSX Manager instances for which you want to import endpoints are up and running.

Procedure

1 Log in or SSH as root to the OS of the VMware Cloud Director cell.

2 Run the command in the following form.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs options
```

Table 5-9. Cell Management Tool Options and Arguments, `trust-infra-certs` Subcommand

Option	Argument	Description
`--help (-h)`	None	Provides a summary of available commands in this category.
`--vsphere`	None	Prompts you to trust certificates for all registered vCenter Server, NSX Data Center for vSphere, and NSX-T Data Center instances in this installation.
`--trust`	None	Optional. Adds certificates to the VMware Cloud Director truststore.
`--inspect`	Optional. File path.	Optional. Displays the certificates into a file.
`--unattended`	None	Optional. The command does not prompt for further input when invoked with this option. All infrastructure certificates are automatically trusted.

Example: Trust and Import All Certificates from vSphere Resources Endpoints

To trust and import the certificates from your vSphere resources endpoints without being prompted for further input, run the command with the following options.

```
/opt/vmware/vcloud-director/bin/cell-management-tool trust-infra-certs --vsphere --unattended
```

Configure a Test Connection Denylist

After installation or upgrade, use the `manage-test-connection-blacklist` command of the cell management tool to block access to internal hosts before providing tenants with access to the VMware Cloud Director network.

Starting with VMware Cloud Director 10.1, service providers and tenants can use the VMware Cloud Director API to test connections to remote servers and to verify the server identity as part of an SSL handshake.

To protect the internal network in which a VMware Cloud Director instance is deployed from malicious attacks, system providers can configure a denylist of internal hosts that are unreachable to tenants.

This way, if a malicious attacker with tenant access attempts to use the connection testing VMware Cloud Director API to map the network in which VMware Cloud Director is installed, they won't be able to connect to the internal hosts on the denylist.

After installation or upgrade and before providing tenants with access to the VMware Cloud Director network, use the `manage-test-connection-blacklist` command of the cell management tool to block tenant access to internal hosts.

Procedure

1 Log in or SSH as root to the OS of the VMware Cloud Director cell.

2 Run the command to add an entry to the denylist.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-test-connection-blacklist
option
```

Table 5-10. Cell Management Tool Options and Arguments, `manage-test-connection-blacklist` Subcommand

Option	Argument	Description
`--help (-h)`	None	Provides a summary of available commands in this category.
`--add-ip`	IPv4 or IPv6 address	Adds an IP address to the denylist.
`--add-name`	A subdomain or a fully qualified domain name for a host	Adds a subdomain or a domain name to the denylist.
`--add-range`	IPv4 or IPv6 address range in either CIDR or hyphenated format	Adds an IP address range to the denylist.
`--list`	None	Lists all the existing entries with denied access.

View the FIPS Status of All Active Cells

Starting with VMware Cloud Director 10.2.2, to verify the FIPS status of all active VMware Cloud Director cells, you can use the `fips-status` command. The command does not show the FIPS status of the VMware Cloud Director appliance.

For more information about enabling FIPS mode for VMware Cloud Director on Linux, see Enable FIPS Mode in the *VMware Cloud Director Service Provider Admin Portal Guide*.

The `fips-status` command displays the FIPS status information for all active cells, including the cell name, UUID, IP address, and FIPS status.

For appliance FIPS mode information, see View the VMware Cloud Director Appliance FIPS Mode.

To receive the data in JSON format, you can specify the `--json` flag.

Procedure

1 Log in directly or by using an SSH client to the OS of the VMware Cloud Director cell as **root**.

2 View the FIPS status of all active cells.

```
/opt/vmware/vcloud-director/bin/cell-management-tool fips-status
```

Table 5-11. Cell Management Tool Options and Arguments, `fips-status` Command

Command	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--json`	None	Displays the information in JSON format.

Managing the List of Allowed SSL Ciphers

Use the `ciphers` command of the cell management tool to configure the set of cipher suites that the cell offers to use during the SSL handshake process.

Note The `ciphers` command only applies to the set of certificates that VMware Cloud Director uses for HTTPS and console proxy communications, and not to the certificates that the VMware Cloud Director appliance uses for its appliance management user interface and API.

When a client makes an SSL connection to a VMware Cloud Director cell, the cell offers to use only those ciphers that are configured on its default list of allowed ciphers. Several ciphers are not on this list, either because they are not strong enough to secure the connection, or because they are known to contribute to SSL connection failures.

When you install or upgrade VMware Cloud Director, the installation or upgrade script examines the cell's certificates. If any of the certificates are encrypted using a cipher that is not on the list of allowed ciphers, the installation or the upgrade fails. You can take the following steps to replace the certificates and reconfigure the list of allowed ciphers:

1 Create certificates that do not use any of the disallowed ciphers. You can use `cell-management-tool ciphers -a` as shown in the example below to list all the ciphers that are allowed in the default configuration.

2 Use the `cell-management-tool certificates` command to replace the cell's existing certificates with the new ones.

3 Use the `cell-management-tool ciphers` command to reconfigure the list of allowed ciphers and to include all necessary ciphers for use with the new certificates.

Important Because the VMRC console requires the use of the AES256-SHA and AES128-SHA ciphers, you cannot disallow them if your VMware Cloud Director clients use the VMRC console.

To manage the list of allowed SSL ciphers, use a command line with the following form:

```
cell-management-tool ciphers options
```

Table 5-12. Cell Management Tool Options and Arguments, `ciphers` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--all-allowed` (-a)	None	List all ciphers that VMware Cloud Director supports.
`--compatible-reset` (-c) (Deprecated)	None	Deprecated. Use the `--reset` option to reset to the default list of allowed ciphers.
`--disallow` (-d)	Comma-separated list of cipher names.	Disallow the ciphers in specified comma-separated list. Every time you run this option, you must include the full list of ciphers you want to deactivate because running the option overwrites the previous setting. **Important** Running the option without any values activates all ciphers. To view all possible ciphers, run the `-a` option. **Important** You must restart the cell after running **`ciphers --disallow`**.

Table 5-12. Cell Management Tool Options and Arguments, `ciphers` Subcommand (continued)

Option	Argument	Description
`--list` (-l)	None	List the set of allowed ciphers that are currently in use.
`--reset` (-r)	None	Reset to the default list of allowed ciphers. If this cell's certificates use disallowed ciphers, you cannot make an SSL connection to the cell until you install new certificates that use an allowed cipher. **Important** You must restart the cell after running **`ciphers --reset`**.

Example: Disallow Two Ciphers

VMware Cloud Director includes a preconfigured list of enabled ciphers.

This example shows how to enable additional ciphers from the list of allowed ciphers and how to disallow ciphers that you don't want to use.

1 Obtain the list of the ciphers that are enabled by default.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -l
```

The output of the command returns the list of enabled ciphers.

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
```

2 Obtain a list of all the ciphers that the cell can offer during an SSL handshake.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
```

The output of the command returns the list of allowed ciphers.

```
# ./cell-management-tool ciphers -a
Product default ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
```

```
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
```

3 Specify which ciphers to deactivate.

If you run the command and you don't explicitly deactivate a cipher, it becomes activated.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool ciphers -d
TLS_RSA_WITH_AES_128_CBC_SHA,TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
```

4 Run the command to check the list of activated ciphers. Any cipher that is absent from the list is deactivated.

```
root@bos1-vcd-static-211-90 [ /opt/vmware/vcloud-director/bin ]# ./cell-management-tool
ciphers -l
```

The output returns a list of all the ciphers that are now enabled.

```
Allowed ciphers:
* TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
* TLS_RSA_WITH_AES_256_GCM_SHA384
* TLS_RSA_WITH_AES_128_GCM_SHA256
* TLS_RSA_WITH_AES_256_CBC_SHA256
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA256
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
```

Manage the List of Allowed SSL Protocols

To configure the set of SSL protocols that the cell offers to use during the SSL handshake process, use the `ssl-protocols` command of the cell management tool.

When a client makes an SSL connection to a VMware Cloud Director cell, the cell offers to use only those protocols that are configured on its list of allowed SSL protocols. Several protocols, including TLSv1, SSLv3, and SSLv2Hello, are not on the default list because they are known to have serious security vulnerabilities.

Procedure

1 Log in directly or by using an SSH client to the OS of the VMware Cloud Director cell as **root**.

2 Run the command to manage the list of allowed SSL protocols.

```
cell-management-tool ssl-protocols options
```

Table 5-13. Cell Management Tool Options and Arguments, `ssl-protocols` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--all-allowed` (-a)	None	List all SSL protocols that VMware Cloud Director supports.
`--disallow` (-d)	Comma-separated list of SSL protocol names.	Reconfigure the list of disallowed SSL protocols to the ones specified in the list. Every time you run this option, you must include the full list of SSL protocols you want to deactivate because running the option overwrites the previous setting. **Important** Running the option without any values activates all SSL protocols. To view all possible SSL protocols, run the `-a` option. **Important** You must restart the cell after running **`ssl-protocols --disallow`**.

Table 5-13. Cell Management Tool Options and Arguments, `ssl-protocols` Subcommand (continued)

Option	Argument	Description
`--list` (-l)	None	List the set of allowed SSL protocols that are currently in use.
`--reset` (-r)	None	Reset the list of configured SSL protocols to the factory default. **Important** You must restart the cell after running **`ssl-protocols --reset`**.

Example: List Allowed and Configured SSL Protocols and Reconfigure the List of Disallowed SSL Protocols

Use the `--all-allowed` (`-a`) option to list all the SSL protocols that the cell can be allowed to offer during an SSL handshake.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

    * TLSv1.2
    * TLSv1.1
    * TLSv1
    * SSLv3
    * SSLv2Hello
```

This list is typically a superset of the SSL protocols that the cell is configured to support. To list those SSL protocols, use the `--list` (-l) option.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

    * TLSv1.2
    * TLSv1.1
```

To reconfigure the list of disallowed SSL protocols, use the `--disallow` (`-d`) option. This option requires a comma-separated list of the subset of allowed protocols produced by `ssl-protocols -a`.

This example updates the list of allowed SSL protocols to include TLSv1. vCenter Server releases earlier than 5.5 Update 3e require TLSv1.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d
SSLv3,SSLv2Hello
```

You must restart the cell after running this command.

Configure Metrics Collection and Publishing

You can use the `configure-metrics` command of the cell management tool to configure the set of metrics to collect.

VMware Cloud Director can collect metrics that provide current and historic information about the virtual machine performance and resource consumption. Use this subcommand to configure the metrics that VMware Cloud Director collects. Use the `cell-management-tool cassandra` subcommand to configure an Apache Cassandra database for use as a VMware Cloud Director metrics repository. See Configuring a Cassandra Metrics Database.

Procedure

1 Log in directly or by using an SSH client to the OS of the VMware Cloud Director cell as **root**.

2 Configure the metrics that VMware Cloud Director collects.

```
/opt/vmware/vcloud-director/bin/cell-management-tool configure-metrics --metrics-config pathname
```

Table 5-14. Cell Management Tool Options and Arguments, `configure-metrics` Subcommand

Command	Argument	Description
`--help (-h)`	None	Provides a summary of available commands in this category.
`--repository-host` (Deprecated)	Host name or IP address of KairosDB host	Deprecated. Use the `--cluster-nodes` option of the `cell-management-tool cassandra` subcommand to configure an Apache Cassandra database for use as a VMware Cloud Director metrics repository.
`--repository-port` (Deprecated)	KairosDB port to use.	Deprecated. Use the `--port` option of the `cell-management-tool cassandra` subcommand to configure an Apache Cassandra database for use as a VMware Cloud Director metrics repository.
`--metrics-confg`	path name	Path to the metrics configuration file

3 If your VMware Cloud Director version is 10.2.2 or later, you can also enable the metrics publishing by running the following command.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n statsFeeder.metrics.publishing.enabled -v true
```

Starting with VMware Cloud Director 10.2.2, the metrics publishing is deactivated by default.

Example: Configuring a Metrics Database Connection

This example configures the metrics collection as specified in the file `/tmp/metrics.groovy`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

The VMware Cloud Director metrics collection service implements a subset of the metrics collected by the vSphere Performance Manager. See the vSphere Performance Manager documentation for more information about metric names and collection parameters. The `metrics-config` file cites one or more metric names and provides collection parameters for each cited metric. For example:

```
configuration {
    metric("cpu.usage.average")
    metric("cpu.usagemhz.average")
    metric("cpu.usage.maximum")
    metric("disk.used.latest") {
        currentInterval=300
        historicInterval=300
        entity="VM"
        instance=""
        minReportingInterval=1800
        aggregator="AVERAGE"
    }
}
```

The following metric names are supported.

Table 5-15. Metric Names

Metric Name	Description
`cpu.usage.average`	Host view of this virtual machine's average actively used CPU as a percentage of total available. Includes all cores in all sockets.
`cpu.usagemhz.average`	Host view of this virtual machine's average actively used CPU as a raw measurement . Includes all cores in all sockets.
`cpu.usage.maximum`	Host view of this virtual machine's maximum actively used CPU as a percentage of total available. Includes all cores in all sockets.
`mem.usage.average`	Memory used by this virtual machine as a percentage of total configured memory.
`disk.provisioned.latest`	Storage space allocated to this virtual hard disk in the containing organization virtual data center.
`disk.used.latest`	Storage used by all virtual hard disks.

Table 5-15. Metric Names (continued)

Metric Name	Description
`disk.read.average`	Average read rate for all virtual hard disks.
`disk.write.average`	Average write rate for all virtual hard disks.

Note When a virtual machine has multiple disks, VMware Cloud Director reports metrics as an aggregate for all disks. CPU metrics are an aggregate of all cores and sockets.

For each named metric, you can specify the following collection parameters.

Table 5-16. Metrics Collection Parameters

Parameter Name	Value	Description
`currentInterval`	Integer number of seconds	The interval in seconds to use when querying for the latest available metric values for current metrics queries. The default value is `20`. VMware Cloud Directorsupports values greater than 20 only for Level 1 metrics, as defined by the vSphere Performance Manager.
`historicInterval`	Integer number of seconds	The interval in seconds to use when querying for historic metric values. The default value is `20`. VMware Cloud Director supports values greater than 20 only for Level 1 metrics, as defined by the vSphere Performance Manager.
`entity`	One of: `HOST`, `VM`	The type of VC object that the metric is available for. The default is `VM`. Not all metrics are available for all entities.
`instance`	A vSphere Performance Manager `PerfMetricId` instance identifier	Indicates whether to retrieve data for individual instances of a metric, for example, individual CPU cores, an aggregate of all instances, or both. A value of `"*"` collects all metrics, instance and aggregate. An empty string, `""` collects only the aggregate data. A specific string like `"DISKFILE"` collects data only for that instance. The default is `"*"`.
`minReportingInterval`	Integer number of seconds	Specifies a default aggregation interval in seconds to use when reporting time series data. Provides further control over reporting granularity when the granularity of the collection interval is not sufficient. The default is `0`, that is, no dedicated reporting interval.
`aggregator`	One of: `AVERAGE`, `MINIMUM`, `MAXIMUM`, `SUMMATION`	The type of aggregation to perform during the `minReportingInterval`. The default is `AVERAGE`.

Configuring a Cassandra Metrics Database

Use the `cassandra` command of the cell management tool to connect the cell to an optional metrics database.

VMware Cloud Director can collect metrics that provide current and historic information about virtual machine performance and resource consumption. Use this subcommand to configure an Apache Cassandra database for use as a VMware Cloud Director metrics repository. Use the `cell-management-tool configure-metrics` subcommand to tool to configure the set of metrics to collect. See Configure Metrics Collection and Publishing.

Data for historic metrics is stored in an Apache Cassandra database. See Install and Configure a Cassandra Database for Storing Historic Metric Data for more information about configuring optional database software to store and retrieve performance metrics.

To create a connection between VMware Cloud Director and an Apache Cassandra database, use a command line with the following form:

```
cell-management-tool cassandra options
```

Table 5-17. Cell Management Tool Options and Arguments, `cassandra` Subcommand

Command	Argument	Description
`--help` (-h)	None	Provides a summary of available options for this command.
`--add-rollup`	None	Updates the metrics schema to include rolled-up metrics. See Install and Configure a Cassandra Database for Storing Historic Metric Data.
`--cluster-nodes`	*address* [, *address* ...]	Comma-separated list of Cassandra cluster nodes to use for VMware Cloud Director metrics.
`--clean`	None	Remove Cassandra configuration settings from the VMware Cloud Director database.
`--configure`	None	Configure VMware Cloud Director for use with an existing Cassandra cluster.
`--dump`	None	Dump the current connection configuration.
`--keyspace`	string	Set VMware Cloud Director key space name in Cassandra to *string*. Defaults to `vcloud_metrics`.
`--offline`	None	Cofigure Cassandra for use by VMware Cloud Director, but do not test the configuration by connection to VMware Cloud Director.
`--password`	string	Password of Cassandra database user

Table 5-17. Cell Management Tool Options and Arguments, `cassandra` Subcommand (continued)

Command	Argument	Description
`--port`	integer	Port to connect to at each cluster node. Defaults to 9042.
`--ttl`	integer	Retain metrics data for *integer* days. Set *integer* to `0` to retain metrics data forever.
`--update-schema`	None	Initializes the Cassandra schema to hold VMware Cloud Director metrics data.
`--username`	string	User name of the Cassandra database user.

Example: Configuring a Cassandra Database Connection

Use a command like this, where *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
```

You must restart the cell after this command completes.

Recovering the System Administrator Password

If you know the VMware Cloud Director database username and password, you can use the `recover-password` command of the cell management tool to recover the VMware Cloud Director system administrator password.

With the `recover-password` command of the cell management tool, a user who knows the VMware Cloud Director database username and password can recover the VMware Cloud Director system administrator password.

To recover the system administrator password, use a command line with the following form:

```
cell-management-tool recover-password options
```

Table 5-18. Cell Management Tool Options and Arguments, `recover-password` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--dbuser`	The user name of the VMware Cloud Director database user.	Must be supplied on the command line.
`--dbpassword`	The password of the VMware Cloud Director database user.	Prompted for if not supplied.

Update the Failure Status of a Task

Use the `fail-tasks` command of the cell management tool to update the completion status associated with tasks that were running when the cell was deliberately shut down. You cannot use the `fail-tasks` command unless all cells have been shut down.

When you quiesce a cell using the `cell-management-tool -q` command, running tasks should terminate gracefully within a few minutes. If tasks continue to run on a cell that has been quiesced, the superuser can shut down the cell, which forces any running tasks to fail. After a shutdown that forced running tasks to fail, the superuser can run `cell-management-tool fail-tasks` to update the completion status of those tasks. Updating a task's completion status in this way is optional but helps maintain the integrity of system logs by clearly identifying failures caused by an administrative action.

To generate a list of tasks that are still running on a quiesced cell, use a command line with the following form:

```
cell-management-tool -u sysadmin-username cell --status-verbose
```

Table 5-19. Cell Management Tool Options and Arguments, `fail-tasks` Subcommand

Command	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--message` (-m)	Message text.	Message text to place in task completion status.

Example: Fail Tasks Running on the Cell

This example updates the task completion status associated with a task that was still running when the cell was shut down.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool fail-tasks -m
"administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system,
Organization: org1
Would you like to fail the tasks listed above?
```

Type **y** to update the task with a completion status of **administrative shutdown**. Type **n** to allow the task to continue running.

Note If multiple tasks are returned in the response, you must decide to fail all of them or take no action. You cannot choose a subset of tasks to fail.

Configure Audit Message Handling

Use the `configure-audit-syslog` command of the cell management tool to configure the way the system logs audit messages.

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

The system configuration script allows you to specify how audit messages are handled. See "Configure Network and Database Connections" in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*. The logging options you specify during system configuration are preserved in two files: `global.properties` and `responses.properties`. You can change the audit message logging configuration in both files with a cell management tool command line of the following form:

```
cell-management-toolconfigure-audit-syslog options
```

Any changes you make with this cell management tool subcommand are preserved in the cell's `global.properties` and `responses.properties` files. Changes do not take effect until you re-start the cell.

Table 5-20. Cell Management Tool Options and Arguments, `configure-audit-syslog` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--disable` (-d)	None	Deactivate logging of audit e vents to `syslog`. Log audit events only to the VMware Cloud Director database. This option unsets the values of the`audit.syslog.host` and `audit.syslog.port` properties in `global.properties` and `responses.properties`.

Table 5-20. Cell Management Tool Options and Arguments, `configure-audit-syslog` Subcommand (continued)

Option	Argument	Description
`--syslog-host` (-loghost)	IP address or fully-qualified domain name of the syslog server host	This option sets the value of the `audit.syslog.host` property to the specified address or fully-qualified domain name.
`--syslog-port` (-logport)	integer in the range 0-65535	This option sets the value of the `audit.syslog.port` property to the specified integer.

When you specify a value for `--syslog-host`, `--syslog-port`, or both, the command validates that the specified value has the correct form but does not test the combination of host and port for network accessibility or the presence of a running `syslog` service.

Example: Change the Syslog Server Host Name

Important Changes you make using this command are written to the global configuration file and the response file. Before you use this command, be sure that the response fine is in place (in `/opt/vmware/vcloud-director/etc/responses.properties`) and writeable. See "Protecting and Reusing the Response File" in the *VMware Cloud Director Installation, Configuration, and Upgrade Guide*.

To change the host to which syslog messages are sent, use a command like this one:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool configure-audit-syslog
-loghost syslog.example.com
Using default port 514
```

This example assumes that the new host listens for syslog messages on the default port.

The command updates `global.properties` and `responses.properties`, but the changes do not take effect until you re-start the cell.

Configuring Email Templates

To manage the templates that the system uses when creating email alerts, you can use the `manage-email` command of the cell management tool.

By default, the system sends email alerts that notify system administrators of events and conditions that are likely to require their intervention. The list of email recipients can be updated using the VMware Cloud Director API or the Web console. You can override the default email content for each kind of alert by using a cell management tool command line of the following form:

```
cell-management-tool manage-email  options
```

Table 5-21. Cell Management Tool Options and Arguments, `manage-email` Subcommand

Option	Argument	Description
`--help`	None	Provides a summary of available commands in this category.
`--delete`	template name	The name of the template to delete.
`--lookup`	template name	This argument is optional. If you do not supply it, the command returns a list of all template names.
`--locale`	the template locale	By default, this command operates on templates in the en-US locale. To specify a different locale, use this option.
`--set-template`	path name to a file containing an updated email template	This file must be accessible on the local host and readable by the user vcloud.vcloud. For example, /tmp/my-email-template.txt

There are different allowed template names that you can use for different email notifications.

Table 5-22. VMware Cloud Director Email Notification Names

Name	Description	When the email is sent	Recipients
`VAPP_UNDEPLOY_NOTIFICATION_SUBJECT` `VAPP_UNDEPLOY_NOTIFICATION_BODY`	Alert when the vApp runtime lease is about to expire. When the lease expires, VMware Cloud Director suspends or powers off the vApp.	Before the runtime lease of a vApp expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
`VAPP_STORAGE_NOTIFICATION_DELETE_SUBJECT` `VAPP_STORAGE_NOTIFICATION_BODY`	Alert when the vApp storage lease is about to expire. When the lease expires, VMware Cloud Director deletes the vApp.	Before the storage lease of a vApp expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
`VAPP_STORAGE_NOTIFICATION_FLAG_SUBJECT` `VAPP_STORAGE_NOTIFICATION_BODY`	Alert when the vApp storage lease is about to expire. When the lease expires, VMware Cloud Director marks the vApp as expired.	Before the storage lease of a vApp expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
`VAPPTEMPLATE_STORAGE_NOTIFICATION_SUBJECT` `VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY`	Alert when the vApp template storage lease is about to expire. When the lease expires, VMware Cloud Director deletes the vApp template.	Before the storage lease of a vApp template expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp Template, or if the owner is a **system administrator**, the **organization administrators** receive the notification.

Table 5-22. VMware Cloud Director Email Notification Names (continued)

Name	Description	When the email is sent	Recipients
VAPPTEMPLATE_STORAGE_NOTIFICATION_SUBJECT VAPPTEMPLATE_STORAGE_NOTIFICATION_BODY	Alert when the vApp template storage lease is about to expire. When the lease expires, VMware Cloud Director marks the vApp template as expired.	Before the storage lease of a vApp template expires, depending on the configured deployment and storage lease alert time.	The owner of the vApp Template, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
DISK_STORAGE_ALERT	Disk Storage Alert (Red Alert)	When there is low disk space on the datastore and it reaches the red threshold.	**System administrators**
DISK_STORAGE_ALERT_VDCS	Disk storage alert to provider VDCs. The email contains the list provider VDCs using the datastore that has a red alert due to low hard disk space.	When there is low disk space on the datastore and it reaches the red threshold.	**System administrators**
VM_HW_UPGRADE_INVALID_POWER_STATE VM_UPDATE_NESTED_HV_INVALID_POWER_STATE	A notification about the power state of a VM. To upgrade the virtual hardware, you must power off the VM.	When a user attempts to upgrade the hardware version of a VM.	The owner of the VM, or if the owner is a **system administrator**, the **organization administrators** receive the notification.
FEDERATION_CERTIFICATE_SUCCESS_SUBJECT FEDERATION_CERTIFICATE_SUCCESS_BODY	Federation certificate expiration notification sent to all **organization administrators** when a certificate for an external SSO server is about to expire. It prompts the **organization administrators** to download a new certificate from the SSO server and update VMware Cloud Director.	If a federation certificate expires within 7 days from the current date.	**Organization administrators**
IPSEC_VPN_TUNNEL_ERROR IPSEC_VPN_TUNNEL_ERROR_SUMMARY	VPN tunnel Error (Red Alert)	When the VPN tunnel is not operational.	**System administrators**
IPSEC_VPN_TUNNEL_ENABLED IPSEC_VPN_TUNNEL_ENABLED _SUMMARY	VPN tunnel Enabled (Green Alert)	When the VPN tunnel is working again after not being operational.	**System administrators**

Table 5-23. Non-customizable Email Templates

Notification	When the email is sent	Recipients
Reconnected vCenter Server email alert	When a vCenter Server is reconnected.	**System administrators**
Disconnected vCenter Server email alert. The email states whether an error or a user request caused the disconnecting of the vCenter Server.	When a vCenter Server is disconnected.	**System administrators**
AMQP Connection Lost email alert. Alert notifying that VMware Cloud Director is disconnected from the AMQP Server.	When the RabbitMQ stops working.	**System administrators**
Broken Database Connection email alert	When VMware Cloud Director is disconnected from the database.	**System administrators**
Restored Database Connection email alert	When VMware Cloud Director is reconnected to the database.	**System administrators**
Host Disconnected from Switch email alert	When a host gets disconnected from the available switches.	**System administrators**
Host Disconnected from Distributed Virtual Switch email alert	When a host gets disconnected from the available distributed virtual switches.	**System administrators**
LDAP Error email alert	During the synchronization with LDAP.	**System administrators**
LDAP User Sync email alert	During the renaming of an LDAP user.	**System administrators**
Site Associations Status Change email alert	The sites recently lost connection, regained connection, or are still down.	**System administrators**

Example: Update an Email Template

The following command replaces the current contents of the DISK_STORAGE_ALERT_VDCS email template with content you created in a file named `/tmp/DISK_STORAGE_ALERT_VDCS-new.txt`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-email --set-
template DISK_STORAGE_ALERT_VDCS /tmp/DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s):
$pvdcsList
"
Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from
$productName The $datastore is used by the followingProvider VDC(s): $pvdcsList
"

VCD Email notification details:
 name                      : DISK_STORAGE_ALERT_VDCS
```

```
 description              : Alert when used disk storage exceeds threshold
 config key               : email.template.DISK_STORAGE_ALERT_VDCS.en-US
 template placeholders    : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcsList]
 template content         : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcsList
```

Finding Orphaned VMs

Use the `find-orphan-vms` command of the cell management tool to find references to virtual machines that are present in the vCenter database but not in the VMware Cloud Director database.

Virtual machines that are referenced in the vCenter database but not in the VMware Cloud Director database are considered orphan VMs because VMware Cloud Director cannot access them even though they may be consuming compute and storage resources. This kind of reference mismatch can arise for a number of reasons, including high-volume workloads, database errors, and administrative actions. The `find-orphan-vms` command enables an administrator to list these VMs so that they can be removed or re-imported into VMware Cloud Director. This command has provisions for specifying an alternate trust store, which might be needed if you are working with VMware Cloud Director or vCenter installations that use self-signed certificates.

Use a command with the following form:

```
cell-management-tool find-orphan-vms options
```

Table 5-24. Cell Management Tool Options and Arguments, `find-orphan-vms` Subcommand

Option	Argument	Description
`--help` (-h)	None	Provides a summary of available commands in this category.
`--enableVerifyHostname`	None	Enable the host name verification part of the SSL handshake.
`--host`	Required	IP address or fully-qualified domain name of the VMware Cloud Director installation to search for orphan VMs.
`--output-file`	path name or -	Full path name of the file to which the list of orphan VMs should be written. Specify a path name of - to write the list to the standard output.
`--password` (-p)	Required	VMware Cloud Director system administrator password.

Table 5-24. Cell Management Tool Options and Arguments, `find-orphan-vms` Subcommand (continued)

Option	Argument	Description
`--port`	VMware Cloud Director HTTPS port.	Specify this only if you do not want this command to use the default VMware Cloud Director HTTPS port.
`--trustStore`	Full path name to a Java trust store file.	Specify this only if you do not want this command to use the default VMware Cloud Director trust store file.
`--trustStorePassword`	Password to specified `--trustStore`	Required only if you use `--trustStore` to specify an alternate trust store file.
`--trustStoreType`	The type of the specified `--trustStore` (PKCS12, JCEKS, ...)	Required only if you use `--trustStore` to specify an alternate trust store file.
`--user` (-u)	Required	VMware Cloud Director system administrator user name.
`--vc-name`	Required	Name of vCenter to search for orphan VMs.
`--vc-password`	Required	vCenter administrator password.
`--vc-user`	Required	vCenter administrator user name.

Example: Finding Orphaned VMs

This example queries a single vCenter server. Because `--output-file` is specified as -, results are returned on the standard output.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vms \
 --host 10.20.30.40 -u vcadmin -vc-name vcenter1 -vc-password P@55w0rd --vc-user admin --
output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc<->resource pool mappings associated with VC: 10.20.30.40 (https://
10.20.30.40:443)
Querying all vdc<->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...)
[moref: "resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test
VMs", parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test
VMs", parent moref : "group-v30533")
```

Join or Leave the VMware Customer Experience Improvement Program

To join or leave the VMware Customer Experience Improvement Program (CEIP), you can use the `configure-ceip` subcommand of the cell management tool.

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.

```
cell-management-tool configure-ceip options
```

If you prefer not to participate in VMware's CEIP for this product, run this command with the `--disable` option.

Table 5-25. Cell Management Tool Options and Arguments, `configure-ceip` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available commands in this category.
`--disable`	None	Leaves the VMware Customer Experience Improvement Program.
`--enable`	None	Joins the VMware Customer Experience Improvement Program.
`--status`	None	Displays the current participation status in the VMware Customer Experience Improvement Program.

Example: Leave the VMware Customer Experience Improvement Program

To leave the VMware Customer Experience Improvement Program, use a command like this one:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --disable
Participation disabled
```

After you run this command, the system no longer sends any information to the VMware Customer Experience Improvement Program.

To confirm the current participation status in the VMware Customer Experience Improvement Program, use a command like this one:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --status
Participation disabled
```

Updating Application Configuration Settings

With the `manage-config` subcommand of the cell management tool, you can update different application configuration settings such as catalog throttling activities.

Table 5-26. Cell Management Tool Options and Arguments, `manage-config` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available options with this subcommand.
`--delete` (`-d`)	None	Removes the target configuration setting.
`--lookup` (`-l`)	None	Look up the value of the target configuration setting.
`--name` (`-n`)	Configuration setting name	The name of the target configuration setting. Required with options `-d`, `-l`, and `-v`.
`--value` (`-v`)	Configuration setting value	Adds or updates the value for the target configuration setting.

For example, you can use the `manage-config` subcommand for Configuring Catalog Synchronization Throttling.

Configuring Catalog Synchronization Throttling

When you have many catalog items published to or subscribed from other organizations, to avoid overloading the system during catalog synchronizations, you can configure catalog synchronization throttling. You can use the `manage-config` subcommand of the cell management tool to configure catalog synchronization throttling by limiting the number of library items that can be synced at the same time.

When a subscribed catalog initiates a catalog synchronization, the published catalog first downloads the library items from the vCenter Server repository to the VMware Cloud Director transfer service storage, then creates download links for the subscribed catalog. You can limit the number of library items that all published catalogs can download at the same time. You can limit the number of library items that all subscribed catalogs can sync at the same time. You can limit the number of library items that a single subscribed catalog can sync at the same time.

You can use the `manage-config` subcommand of the cell management tool to update the configuration settings for catalog throttling. For information about using the `manage-config` subcommand, see Updating Application Configuration Settings.

Table 5-27. Configuration Settings for Catalog Throttling

Configuration Setting	Default Value	Description
`vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit`	30	The limit of library items that all published catalogs in the VMware Cloud Director instance can download from vCenter Server to VMware Cloud Director at the same time. If the total number of published library items for downloading across the VMware Cloud Director instance is greater than this limit, the library items are divided into portions by this limit and downloaded in a sequence.
`vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit`	30	The limit of library items that all subscribed catalogs in a VMware Cloud Director instance can sync at the same time. If the total number of subscribed library items for syncing across the VMware Cloud Director instance is greater than this limit, the items are divided into portions by this limit and synced in a sequence.
`contentLibrary.item.sync.batch.size`	10	The limit of library items that a single subscribed catalog can sync at the same time. If a subscribed catalog tries to sync a number of library items that is greater than this limit, the items are divided into portions by this limit and synced in a sequence.

Example: Configuring Synchronization Throttling for Subscribed Catalogs

The following command sets a limit of five for the library items that a single subscribed catalog can sync at the same time.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
contentLibrary.item.sync.batch.size -v 5
```

If a subscribed catalog contains 13 library items, syncing the catalog is performed in three sequential portions. The first portion contains five items, the second portion contains the next five items, the last portion contains the remaining three items.

Troubleshoot Failed Access to the VMware Cloud Director User Interface

To view and update the valid IP addresses and DNS entries for the VMware Cloud Director cells in your VMware Cloud Director environment, you can use the `manage-config` subcommand of the cell management tool.

Problem

You cannot access the VMware Cloud Director Service Provider Admin Portal or the VMware Cloud Director Tenant Portal after a successful login.

After you enter your credentials in the login screen, the following error message is displayed: `Failed to Start. An error was encountered during initialization. This can be caused by issues such as accessing the application via an unsupported public URL or poor connectivity.`

Cause

VMware Cloud Director uses a Cross-Origin Resource Sharing (CORS) filter implementation to maintain a list of all valid endpoints that you can use to access the Service Provider Admin Portal and the VMware Cloud Director Tenant Portal.

The CORS filtering list is populated and updated during the cell configuration. It contains HTTP and HTTPS entries with IP addresses and DNS names for all cells in the server group. It also contains a public IP address that is used by the load balancer which fronts the VMware Cloud Director server group.

During the cell configuration of appliance deployments, the list is not updated with the DNS names of the VMware Cloud Director cells, and you cannot use the DNS name of a cell to access it.

Solution

1. Log in or SSH as **root** to one of the cells in the server group.
2. To list the valid URLs that you can use to access the VMware Cloud Director cells in your environment, run the following command line.

   ```
   [root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n webapp.allowed.origins -l
   ```

   The system output is a list that contains HTTP and HTTPS entries with IP addresses and DNS names for all cells in the server group. It also contains a public IP address that is used by the load balancer which fronts the VMware Cloud Director server group.

   The list is a comma-separated string, without spaces between the entries.

3 (Optional) To update the `webapp.allowed.origins` configuration setting, run the following command line. In the command line, the value parameter of the setting is a list of IP addresses and DNS names in a comma-separated string without spaces between the entries.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
webapp.allowed.origins -v "comma_separated_list_of_URLs_without_spaces"
```

Debugging vCenter VM Discovery

By using the `debug-auto-import` subcommand of the cell management tool, you can investigate the reason for which the mechanism for discovering vApps skips one or more vCenter VMs.

In the default configuration, an organization VDC automatically discovers vCenter VMs that are created in the resource pools that back the VDC. See the discovering and adopting vApps information in the *VMware Cloud Director Service Provider Admin Portal Guide*. If a vCenter VM does not appear in a discovered vApp, you can run the `debug-auto-import` subcommand against this VM or VDC.

```
cell-management-tool debug-auto-import options
```

The `debug-auto-import` subcommand returns a list of vCenter VMs and information about the possible reasons for being skipped by the discovery mechanism. The list also includes vCenter VMs that are discovered but failed to import to the organization VCD.

Table 5-28. Cell Management Tool Options and Arguments, `debug-auto-import` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available commands in this category.
`--org`	Organization name	Optional. Lists information about the skipped VMs for the specified organization.
`--vm`	VM name or part of a VM name	Lists information about the skipped VMs that contain the specified VM name. Optional if the `--org` option is used.

Example: Debug vCenter VM Discovery by VM Name `test`

The following command returns information about skipped vCenter VMs across all organizations.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc
can be skipped for the following reasons:
1) Virtual machine is already imported in vCD or is managed by vCD
2) Virtual machine is created by vCD

VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc
can be skipped for the following reasons:
1) Virtual machine is not present in a vCD managed resource pool

VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry
```

In this example, the system output returns information about three vCenter VMs that are skipped by the discovery mechanism and whose names contain the string `test`. VM `import-test3` is an example of a VM that is discovered but failed to import to the VDC.

Regenerating MAC Addresses for Multisite Stretched Networks

If you associate two VMware Cloud Director sites that are configured with the same installation ID, you might encounter MAC address conflicts in stretched networks across these sites. To avoid such conflicts, you must regenerate the MAC addresses in one of the sites based on a custom seed that is different from the installation ID.

During the initial VMware Cloud Director setup, you set an installation ID. VMware Cloud Director uses the installation ID to generate MAC addresses for the virtual machine network interfaces. Two VMware Cloud Director installations that are configured with the same installation ID might generate identical MAC addresses. Duplicate MAC addresses might cause conflicts in stretched networks between two associated sites.

Before creating stretched networks between associated sites that are configured with the same installation ID, you must regenerate the MAC addresses in one of the sites by using the `mac-address-management` subcommand of the cell management tool.

```
cell-management-tool mac-address-management options
```

To generate new MAC addresses, you set a custom seed that is different from the installation ID. The seed does not overwrite the installation ID, but the database stores the latest seed as a second configuration parameter, which overrides the installation ID.

You run the `mac-address-management` subcommand from an arbitrary VMware Cloud Director member of the server group. The command runs against the VMware Cloud Director database, so you run the command once for a server group.

Important The MAC addresses regeneration requires some downtime of VMware Cloud Director. Before starting the regeneration, you must quiesce the activities on all cells in the server group.

Table 5-29. Cell Management Tool Options and Arguments, `mac-address-management` Subcommand

Option	Argument	Description
`--help` (`-h`)	None	Provides a summary of available commands in this category.
`--regenerate`	None	Deletes all MAC addresses that are not in use and generates new MAC addresses based on the current seed. If there is no a previously set seed, the MAC addresses are regenerated based on the installation ID. The MAC addresses that are in use are retained. **Note** All cells in the server group must be inactive. For information about quiescing the activities on a cell, see Managing a Cell.
`--regenerate-with-seed`	A seed number from 0 to 63	Sets a new custom seed in the database, deletes all MAC addresses that are not in use, and generates new MAC addresses based on the newly set seed. The MAC addresses that are in use are retained. **Note** All cells in the server group must be inactive. For information about quiescing the activities on a cell, see Managing a Cell.
`--show-seed`	None	Returns the current seed and the number of MAC addresses that are in use for each seed.

Important The MAC addresses that are in use are retained. To change a MAC address that is in use to a regenerated MAC address, you must reset the network interface MAC address. For information about editing virtual machine properties, see the *VMware Cloud Director Tenant Portal Guide*.

Example: Regenerating the MAC Addresses Based on a New Custom Seed

The following command sets the current seed to *9* and regenerates all MAC addresses that are not use based on the newly set seed:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses.
Successfully generated new MAC addresses.
```

Example: Viewing the Current Seed and the Number of MAC Addresses in Use for Each Seed

The following command returns information about the current seed and number of MAC addresses per seed:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --show-seed
Current MAC address seed is '9' and based on MacAddressSeed config.
MAC address seed    9 is in use by     12 MAC addresses
MAC address seed    1 is in use by      1 MAC addresses
```

In this example, the system output shows that the current seed is 9, based on which there are 12 MAC addresses. In addition, there is one MAC address that is based on a previous seed or installation ID of 1.

Update the Database IP Addresses on VMware Cloud Director Cells

To update the IP addresses of the VMware Cloud Director cells in a database high availability cluster, you can use the cell management tool.

Prerequisites

To update the IP addresses of the cells in a database high availability cluster, you must provide the IP address of the current primary. To find the IP address, you must use the VMware Cloud Director appliance API to make a note of the node IDs of the standby nodes in the cluster. See the *VMware Cloud Director Appliance API Schema Reference* on http://code.vmware.com.

Procedure

1. Log in directly or by using an SSH client to the OS of any of the cells in the cluster as **root**.
2. Check if the cell is running on that node.

   ```
   service vmware-vcd pid cell
   ```

   If the cell process ID is not NULL, the VMware Cloud Director cell is running and you can change the IP address of the database without restarting the VMware Cloud Director cell.

3 To update the IP addresses on all the cells in the server group, run the following command:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address --pid cell process ID --remote-sudo-user postgres --private-key-path /opt/vmware/vcloud-director/id_rsa
```

The system output indicates the successful reconfiguration.

4 (Optional) Verify that each VMware Cloud Director cell is pointing to the correct database IP address.

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

The system output indicates that the cell is updated.

5 If any of the cells is not updated, run the command to reconfigure it.

- If the cell is not running, run the following command:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address
```

- If the cell is running, run the following command:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address -i cell process ID
```

6 If you reconfigured a cell that is not running, run the command to restart the `vmware-vcd` service.

a Run the command to stop the service.

```
/opt/vmware/vcloud-director/bin/cell-management-tool cell -i $(service vmware-vcd pid cell) -s
```

b Run the command to start the service.

```
systemctl start vmware-vcd
```

Collect VMware Cloud Director Logs

6

VMware Cloud Director provides logging information for each cloud cell in your server group. You can view the logs to monitor your cells and to troubleshoot any problems that you encounter during the day-to-day running of VMware Cloud Director.

VMware Cloud Director Logs

Log Name File or Directory	Description
`/opt/vmware/vcloud-director/logs/cell.log`	Console output from the VMware Cloud Director cell.
`/opt/vmware/vcloud-director/logs/cell-management-tool`	Cell Management Tool log messages from the cell.
`/opt/vmware/vcloud-director/logs/cell-runtime`	Runtime log messages from the cell.
`/opt/vmware/vcloud-director/logs/cloud-proxy`	Cloud proxy log messages from the cell.
`/opt/vmware/vcloud-director/logs/console-proxy`	Remote console proxy log messages from the cell.
`/opt/vmware/vcloud-director/logs/server-group-communications`	Server group communications from the cell.
`/opt/vmware/vcloud-director/logs/statsfeeder`	Virtual machine metric retrieval from vCenter Server and storage information and error messages.
`/opt/vmware/vcloud-director/logs/vcloud-container-debug.log`	Debug-level log messages from the cell.
`/opt/vmware/vcloud-director/logs/vcloud-container-info.log`	Informational log messages from the cell. This log also shows warnings or errors encountered by the cell.
`/opt/vmware/vcloud-director/logs/vmware-vcd-watchdog.log`	Informational log messages from the cell watchdog. It records when the cell stops responding, is restarted, and so on.
`/opt/vmware/vcloud-director/logs/diagnostics.log`	Cell diagnostics log. This file is empty unless diagnostics logging is enabled in the local logging configuration.
`/opt/vmware/vcloud-director/logs/`*`YYYY_MM_DD`*`.request.log`	HTTP request logs in the Apache common log format.

VMware Cloud Director Appliance Logs

The VMware Cloud Director appliance features some additional log files.

Log file	Description
`/opt/vmware/var/log/firstboot`	Contains logging information related to the first boot of the appliance.
`/opt/vmware/var/log/vcd`	Contains logs related to the Replication Manager (`repmgr`) tool suite setup, reconfiguration, and appliance synchronization.
`/opt/vmware/var/log/vcd/pg`	Contains logs related to the backup of the embedded appliance database.
`/opt/vmware/etc/vami/ovfEnv.xml`	Contains the OVF deployment parameters.
`/var/vmware/vpostgres/current/pgdata/log`	Contains logs related to the embedded PostgreSQL database.
`/opt/vmware/var/log/vami/updatecli.log`	Contains logging related to appliance upgrades.

Use any text editor, text viewer, or third-party tool to view the logs.

Uninstall VMware Cloud Director Software

7

Use the Linux `rpm` command to uninstall VMware Cloud 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 VMware Cloud Director.