

Guía de instalación, configuración y actualización de vCloud Director

28 de marzo de 2019
VMware Cloud Director 9.7

Puede encontrar la documentación técnica más actualizada en el sitio web de VMware:

<https://docs.vmware.com/es/>

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

VMware Spain, S.L.
Calle Rafael Boti 26
2.ª planta
Madrid 28023
Tel.: +34 914125000
www.vmware.com/es

Copyright © 2010-2020 VMware, Inc. Todos los derechos reservados. [Información sobre el copyright y la marca comercial.](#)

Contenido

Guía de instalación, configuración y actualización de vCloud Director 7

Información actualizada 8

1 Descripción general de la instalación, configuración y actualización de vCloud Director 9

Arquitectura de vCloud Director 9

Planificación de la configuración 11

2 Requisitos de hardware y de software de vCloud Director 12

Requisitos de configuración de red para vCloud Director 13

Requisitos de seguridad de red 15

3 Antes de instalar vCloud Director o implementar el dispositivo de vCloud Director 17

Preparar la base de datos de vCloud Director 17

Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux 18

Configurar una base de datos de Microsoft SQL Server externa para vCloud Director en Linux 19

Preparar el almacenamiento del servidor de transferencia 21

Descarga e instalación de la clave pública de VMware 24

Instalar y configurar NSX Data Center for vSphere para vCloud Director 24

Instalar y configurar NSX-T Data Center para vCloud Director 25

4 Creación y administración de certificados SSL para vCloud Director en Linux 27

Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux 27

Crear certificados SSL autofirmados para vCloud Director en Linux 28

Crear un almacén de claves de certificados SSL firmados por una entidad de certificación para vCloud Director en Linux 29

Crear un almacén de claves de certificados SSL firmados por una entidad de certificación con claves privadas importadas para vCloud Director en Linux 33

5 Instalar vCloud Director en Linux 35

Instalar vCloud Director en el primer miembro de un grupo de servidores 36

Configuración de conexiones de red y de base de datos 38

Referencia de configuración interactiva 40

Referencia de configuración sin supervisión 42

Proteger y reutilizar el archivo de respuesta 45

Instalar vCloud Director en un miembro adicional de un grupo de servidores 46

Configurar vCloud Director 48

6 Implementar el dispositivo de vCloud Director 51

Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos 53

Requisitos previos para implementar el dispositivo de vCloud Director 56

Implementar el dispositivo de vCloud Director mediante vSphere Web Client o vSphere Client 56

Iniciar la implementación del dispositivo de vCloud Director 57

Personalizar el dispositivo de vCloud Director y finalizar la implementación 59

Implementar el dispositivo de vCloud Director mediante VMware OVF Tool 62

7 Creación y administración de certificados SSL del dispositivo vCloud Director 69

Implementar el dispositivo de vCloud Director con certificados comodín firmados para las comunicaciones de proxy de consola y HTTPS 69

Crear e importar certificados SSL firmados por una entidad de certificación para el dispositivo de vCloud Director 71

Importar claves privadas y certificados SSL firmados por una entidad de certificación en el dispositivo de vCloud Director 75

Reemplazar un certificado autofirmado de interfaz de usuario de administración de dispositivos de vCloud Director y de una instancia integrada de PostgreSQL 77

Renovar los certificados del dispositivo de vCloud Director 78

8 Configuración del dispositivo de vCloud Director 80

Ver el estado de las celdas en un clúster de alta disponibilidad de la base de datos 80

Recuperarse de un error de base de datos principal en un clúster de alta disponibilidad 81

Copia de seguridad y restauración de la base de datos integrada del dispositivo de vCloud Director 82

Realizar una copia de seguridad de la base de datos integrada del dispositivo de vCloud Director 82

Restaurar un entorno de dispositivo de vCloud Director con una configuración de base de datos de alta disponibilidad 83

Restaurar un entorno de dispositivo de vCloud Director sin una configuración de base de datos de alta disponibilidad 86

Configurar el acceso externo a la base de datos de vCloud Director 89

Habilitar o deshabilitar el acceso SSH al dispositivo de vCloud Director 90

Editar la configuración de DNS del dispositivo de vCloud Director 91

Editar las rutas estáticas de las interfaces de red del dispositivo de vCloud Director 91

Scripts de configuración en el dispositivo de vCloud Director 93

Modificar las configuraciones de PostgreSQL en el dispositivo de vCloud Director 93

9 Usar Replication Manager Tool Suite en la configuración de un clúster de alta disponibilidad 95

Comprobar el estado de conectividad de un clúster de alta disponibilidad de la base de datos 96

- Comprobar el estado de replicación de un nodo en un clúster de alta disponibilidad de la base de datos 97
 - Comprobar el estado de un clúster de alta disponibilidad de la base de datos 98
 - Detectar un nodo principal anterior que vuelve a conectarse en un clúster de alta disponibilidad 99
 - Cambiar las funciones de la celda principal y una celda en espera en un clúster de alta disponibilidad de la base de datos 101
 - Eliminar del registro un nodo en espera con errores o inaccesible en un clúster de alta disponibilidad de la base de datos 103
 - Eliminar del registro una celda principal con errores en un clúster de alta disponibilidad de la base de datos 103
 - Eliminar del registro una celda en espera en ejecución en un clúster de alta disponibilidad de la base de datos 104
- 10 Después de instalar vCloud Director o implementar el dispositivo de vCloud Director 106**
- Instalar archivos de Microsoft Sysprep en los servidores 106
 - Personalizar endpoints públicos 107
 - Instalar y configurar un agente AMQP de RabbitMQ 110
 - Instalar y configurar una base de datos de Cassandra para almacenar datos de métricas históricas 112
 - Realizar configuraciones adicionales en la base de datos externa de PostgreSQL 113
- 11 Actualizar vCloud Director y aplicar revisiones al dispositivo de vCloud Director 116**
- Realizar una actualización orquestada de una instalación de vCloud Director 118
 - Actualizar manualmente una instalación de vCloud Director 121
 - Actualizar una celda de vCloud Director 122
 - Actualización de la base de datos de vCloud Director 125
 - Referencia de la utilidad de actualización de bases de datos 126
 - Aplicar revisiones a la implementación del dispositivo de vCloud Director 129
- 12 Migrar al dispositivo de vCloud Director 132**
- Migrar vCloud Director con una base de datos Microsoft SQL externa al dispositivo de vCloud Director 132
 - Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director 136
- 13 Después de actualizar o migrar vCloud Director 142**
- Actualizar cada instancia de NSX Manager que esté asociada con un sistema vCenter Server adjunto 142
 - Actualizar sistemas vCenter Server, hosts ESXi e instancias de NSX Edge 143
 - Nuevos derechos en esta versión 145
- 14 Solucionar problemas del dispositivo de vCloud Director 146**

[Examinar los archivos de log en el dispositivo de vCloud Director](#) 146

[La celda de vCloud Director no se puede iniciar después de la implementación del dispositivo](#) 147

[Error al volver a configurar el servicio de vCloud Director cuando se realiza una migración al dispositivo de vCloud Director o una restauración en este](#) 148

[Usar los archivos de registro para solucionar problemas de actualizaciones y revisiones de vCloud Director](#) 148

[Error al buscar actualizaciones de vCloud Director](#) 149

[Error al instalar la última actualización de vCloud Director](#) 149

15 Desinstalación del software de vCloud Director 150

Guía de instalación, configuración y actualización de vCloud Director

En *Guía de instalación, configuración y actualización de vCloud Director*, se proporciona información sobre la instalación y la actualización de VMware vCloud Director[®] for Service Providers, así como la configuración para que este software funcione con VMware vSphere[®], VMware NSX[®] for vSphere[®] y VMware NSX-T[™] Data Center.

Público objetivo

La *Guía de instalación, configuración y actualización de vCloud Director* está destinada a cualquiera que quiera instalar o actualizar el software de vCloud Director. La información de esta guía ha sido creada para administradores del sistema con experiencia que están familiarizados con Linux, Windows, redes IP y vSphere.

Información actualizada

Esta documentación sobre *Guía de instalación, configuración y actualización de vCloud Director* se actualiza con cada versión del producto o cuando sea necesario.

En esta tabla se muestra el historial de actualizaciones de *Guía de instalación, configuración y actualización de vCloud Director*.

Revisión	Descripción
11 de junio de 2019	<ul style="list-style-type: none">■ Se agregó el tema Renovar los certificados del dispositivo de vCloud Director.■ Se añadió el capítulo Capítulo 9 Usar Replication Manager Tool Suite en la configuración de un clúster de alta disponibilidad.
10 de mayo de 2019	<ul style="list-style-type: none">■ Se añadió el capítulo #unique_5.■ Se agregó el tema Usar los archivos de registro para solucionar problemas de actualizaciones y revisiones de vCloud Director.■ Se agregó el tema Error al buscar actualizaciones de vCloud Director.■ Se agregó el tema Error al instalar la última actualización de vCloud Director.
5 de abril de 2019	<ul style="list-style-type: none">■ Se añadió el capítulo Capítulo 12 Migrar al dispositivo de vCloud Director.■ Se agregó el tema Restaurar un entorno de dispositivo de vCloud Director con una configuración de base de datos de alta disponibilidad.■ Se actualizó el tema Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos para mejorar los gráficos y el paso 2 de los flujos de trabajo.■ Se actualizó el tema Examinar los archivos de log en el dispositivo de vCloud Director para agregar información sobre el archivo que contiene los parámetros de OVF de la implementación.
28 de marzo de 2019	Versión inicial.

Descripción general de la instalación, configuración y actualización de vCloud Director

1

Para crear un grupo de servidores de vCloud Director, es posible instalar el software de vCloud Director en uno o varios servidores Linux o implementar una o varias instancias del dispositivo de vCloud Director. Durante el proceso de instalación, se realiza la configuración inicial de vCloud Director, incluido el establecimiento de las conexiones de red y de base de datos.

El software vCloud Director para Linux requiere una base de datos externa, mientras que el dispositivo de vCloud Director utiliza una base de datos de PostgreSQL integrada.

Después de crear el grupo de servidores de vCloud Director, es posible integrar la instalación de vCloud Director con los recursos de vSphere. Para los recursos de red, vCloud Director puede usar NSX Data Center for vSphere, NSX-T Data Center o ambos.

Al actualizar una instalación existente de vCloud Director, se actualiza el software de vCloud Director y el esquema de base de datos, pero se mantienen las relaciones existentes entre servidores, base de datos y vSphere.

Cuando se migra una instalación de vCloud Director existente en Linux al dispositivo de vCloud Director, se actualiza el software vCloud Director y se migra la base de datos a la base de datos integrada en el dispositivo.

Este capítulo incluye los siguientes temas:

- [Arquitectura de vCloud Director](#)
- [Planificación de la configuración](#)

Arquitectura de vCloud Director

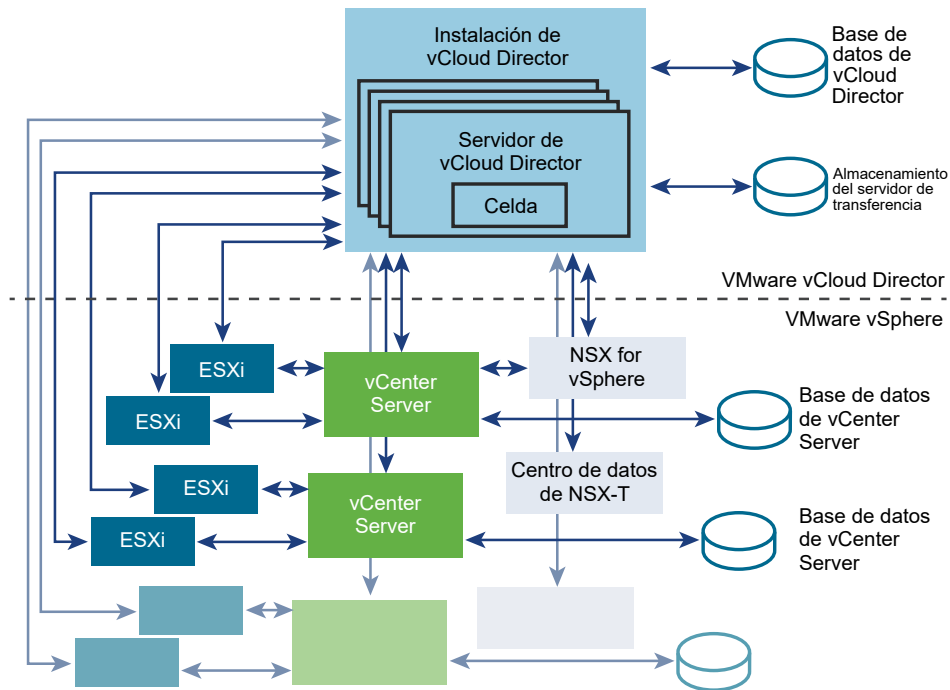
Un grupo de servidores de vCloud Director consta de uno o varios servidores de vCloud Director instalados en Linux o implementaciones del dispositivo de vCloud Director. Cada servidor del grupo ejecuta una colección de servicios denominada celda de vCloud Director. Todas las celdas comparten una sola base de datos de vCloud Director y un almacenamiento del servidor de transferencia, y se conectan a los recursos de red y vSphere.

Importante No se admiten instalaciones mixtas de vCloud Director en implementaciones de Linux y dispositivos de vCloud Director en un grupo de servidores.

Para garantizar la alta disponibilidad de vCloud Director, debe instalar al menos dos celdas de vCloud Director en un grupo de servidores. Si se utiliza un equilibrador de carga de terceros, se puede garantizar una conmutación por error automática sin tiempo de inactividad.

Puede conectar una instalación de vCloud Director con varios sistemas de VMware vCenter Server® y los hosts VMware ESXi™ que administran. En el caso de los servicios de red, vCloud Director puede usar NSX Data Center for vSphere asociado con vCenter Server o puede registrar NSX-T Data Center con vCloud Director. También se admite la combinación de NSX Data Center for vSphere y NSX-T Data Center.

Figura 1-1. Diagrama de la arquitectura de vCloud Director



Un grupo de servidores de vCloud Director instalado en Linux utiliza una base de datos externa.

Un grupo de servidores de vCloud Director que consta de implementaciones de dispositivos utiliza la base de datos integrada en el primer miembro del grupo de servidores. Puede configurar la alta disponibilidad de una base de datos de vCloud Director mediante la implementación de dos instancias del dispositivo como celdas en espera en el mismo grupo de servidores. Consulte [Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos](#).

Figura 1-2. Dispositivos de vCloud Director que constan de un clúster de alta disponibilidad de base de datos integrada

El proceso de instalación y configuración de vCloud Director crea las celdas, las conecta a la base de datos compartida y al almacenamiento del servidor de transferencia, y crea la cuenta de **administrador del sistema**. A continuación, el **administrador del sistema** establece conexiones con el sistema de vCenter Server, los hosts ESXi y las instancias de NSX Manager. Para obtener información sobre cómo agregar recursos de red y vSphere, consulte la *Guía del administrador de vCloud Director*.

Planificación de la configuración

vSphere proporciona capacidad de almacenamiento, cálculo y redes a vCloud Director. Antes de iniciar la instalación, tenga en cuenta la capacidad de vSphere y vCloud Director que necesita la nube, y planee una configuración que pueda dar cabida a la misma.

Los requisitos de configuración dependen de varios factores, incluso la cantidad de organizaciones que haya en la nube, la cantidad de usuarios de cada organización y el nivel de actividad de dichos usuarios. Las directrices siguientes pueden servir como punto de partida para la mayoría de las configuraciones:

- Asigne una celda de vCloud Director por cada sistema vCenter Server que desee que esté disponible en la nube.
- Asegúrese de que todos los servidores Linux de vCloud Director satisfacen al menos los requisitos mínimos de memoria y almacenamiento que se especifican en *Notas de la versión de vCloud Director*.
- Si tiene previsto instalar vCloud Director en Linux, configure la base de datos de vCloud Director como se describe en [Preparar la base de datos de vCloud Director](#).

Requisitos de hardware y de software de vCloud Director

2

Cada servidor de un grupo de servidores de vCloud Director debe cumplir ciertos requisitos de hardware y de software. Además, debe estar disponible una base de datos accesible para todos los miembros del grupo. Cada grupo de servidores requiere acceso a un sistema de vCenter Server, una instancia de NSX Manager y uno o más hosts ESXi.

Compatibilidad con otros productos de VMware

Para obtener la información más reciente acerca de la compatibilidad entre vCloud Director y otros productos de VMware, consulte las *matrices de interoperabilidad de productos de VMware* en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Requisitos de configuración de vSphere

Las instancias de vCenter Server y los hosts ESXi que se pretendan utilizar con vCloud Director deben cumplir requisitos de configuración específicos.

- Las redes de vCenter Server que se pretendan utilizar como redes externas o como grupos de redes de vCloud Director deben estar disponibles para todos los hosts en cualquier clúster destinado al uso de vCloud Director. Al poner dichas redes a disposición de todos los hosts de un centro de datos, se simplifica la tarea de añadir nuevas instancias de vCenter Server a vCloud Director.
- Se requieren conmutadores distribuidos de vSphere para las redes aisladas y los grupos de redes que respalda NSX Data Center for vSphere.
- Los clústeres de vCenter Server usados con vCloud Director deben especificar un nivel de automatización de vSphere DRS **Completamente automatizado**. Storage DRS, si está habilitado, puede configurarse con cualquier nivel de automatización.
- Las instancias de vCenter Server deben confiar en los hosts. Todos los hosts de todos los clústeres gestionados por vCloud Director deben configurarse para exigir certificados de host verificados. En concreto, debe determinar, comparar y seleccionar huellas digitales coincidentes para todos los hosts. Consulte el apartado Configure SSL Settings incluido en el documento *vCenter Server and Host Management*.

Requisitos de licencia de vSphere

vCloud Director Service Provider Bundle incluye las licencias de vSphere necesarias.

Exploradores, bases de datos y plataformas compatibles

Consulte las *Notas de la versión de vCloud Director 9.7* para obtener información acerca de plataformas del servidor, navegadores, servidores de LDAP y bases de datos compatibles con esta versión de vCloud Director.

Requisitos de CPU, memoria y espacio en disco

Los requisitos físicos como CPU, memoria y espacio en disco de las celdas de vCloud Director se enumeran en las *Notas de la versión de vCloud Director 9.7*.

Almacenamiento compartido

NFS u otro volumen de almacenamiento compartido para el servicio de transferencia de vCloud Director. El volumen de almacenamiento debe ser ampliable y accesible para todos los servidores del grupo de servidores.

Este capítulo incluye los siguientes temas:

- [Requisitos de configuración de red para vCloud Director](#)
- [Requisitos de seguridad de red](#)

Requisitos de configuración de red para vCloud Director

El funcionamiento seguro y fiable de vCloud Director depende de que la red sea segura y fiable, y que admita la búsqueda directa e inversa de nombres de host, un servicio de temporización de red y otros servicios. La red debe cumplir estos requisitos para poder empezar la instalación de vCloud Director.

La red que conecta los servidores de vCloud Director, el servidor de base de datos, los sistemas vCenter Server y los componentes de NSX, deben cumplir varios requisitos:

direcciones IP

Cada servidor de vCloud Director debe admitir dos endpoints SSL diferentes. Un endpoint es para el servicio HTTP, mientras que el otro es para el servicio de proxy de la consola. Estos endpoints pueden ser direcciones IP separadas o una única dirección IP con dos puertos diferentes. Puede utilizar alias de IP o varias interfaces de red para crear dichas direcciones. No utilice el comando `ip addr add` de Linux para crear la segunda dirección.

El dispositivo de vCloud Director utiliza la dirección IP de `eth0` con el puerto personalizado 8443 para el servicio de proxy de consola.

Dirección del proxy de consola

La dirección IP configurada como endpoint del proxy de consola no debe estar ubicada detrás de un equilibrador de cargas que finalice en SSL o de un proxy inverso. Todas las solicitudes de proxy de consola se deben retransmitir directamente a la dirección IP del proxy de consola.

En una instalación con una sola dirección IP, puede personalizar la dirección de proxy de la consola desde la consola web de vCloud Director. Por ejemplo, para el dispositivo de vCloud Director, debe personalizar la dirección de proxy de la consola como `vcloud.example.com:8443`.

Servicio de temporización de red

Debe utilizar un servicio de temporización de red, tal como NTP, para sincronizar los relojes de todos los vCloud Director Servers, incluso el servidor de base de datos. La diferencia máxima permitida entre los relojes de los servidores sincronizados es de 2 segundos.

Zona horaria de servidor

Todos los vCloud Director Servers, incluido el servidor de base de datos, deben configurarse para estar en la misma zona horaria.

Resolución de nombres de host

Todos los nombres de host que especifique durante la instalación y configuración deben poder resolverse mediante DNS haciendo uso de búsqueda directa e inversa del nombre de dominio totalmente cualificado o del nombre de host no cualificado. Por ejemplo, para un host denominado `vcloud.example.com`, los dos comandos que figuran a continuación deben ejecutarse correctamente en un host de vCloud Director:

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

Además, si el host `vcloud.example.com` tiene la dirección IP 192.168.1.1, el comando siguiente debe devolver `vcloud.example.com`:

```
nslookup 192.168.1.1
```

La búsqueda de DNS inversa de la dirección IP de `eth0` es obligatoria para el dispositivo. El siguiente comando debe ejecutarse correctamente en su entorno:

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

Requisitos de seguridad de red

El funcionamiento seguro de vCloud Director requiere un entorno de red protegido. Configure y pruebe dicho entorno de red antes de empezar a instalar vCloud Director

Conecte todos los vCloud Director Servers a una red que esté protegida y que se esté supervisando. Las conexiones de red de vCloud Director tienen varios requisitos adicionales:

- No conecte vCloud Director directamente a la red de Internet pública. Siempre proteja las conexiones de red de vCloud Director con un firewall. Solamente el puerto 443 (HTTPS) debe estar abierto para las conexiones entrantes. Los puertos 22 (SSH) y 80 (HTTP) también se pueden abrir para las conexiones entrantes, de ser necesario. Además, `cell-management-tool` requiere acceso a la dirección del bucle invertido de la celda. El firewall debe rechazar el resto del tráfico entrante procedente de redes públicas, incluidas las solicitudes realizadas a JMX (puerto 8999).

Tabla 2-1. Puertos que deben permitir paquetes entrantes provenientes de hosts de vCloud Director

Puerto	Protocolo	Comentarios
111	TCP, UDP	Asignador de puertos NFS utilizado por el servicio de transferencia
920	TCP, UDP	rpc.statd de NFS utilizado por el servicio de transferencia
61611	TCP	AMQP.
61616	TCP	AMQP.

- No conecte a la red pública los puertos utilizados con las conexiones salientes.

Tabla 2-2. Puertos que deben permitir paquetes salientes provenientes de hosts de vCloud Director

Puerto	Protocolo	Comentarios
25	TCP, UDP	SMTP
53	TCP, UDP	DNS
111	TCP, UDP	Asignador de puertos NFS utilizado por el servicio de transferencia
123	TCP, UDP	NTP
389	TCP, UDP	LDAP
443	TCP	Las conexiones de vCenter, NSX Manager y ESXi usan el puerto estándar. Si ha elegido otro puerto para estos servicios, deshabilite la conexión al puerto 443 y habilítelos en el puerto que haya seleccionado.
514	UDP	Opcional. Permite el uso de syslog.
902	TCP	Conexiones de vCenter y de ESXi.
903	TCP	Conexiones de vCenter y de ESXi.

Tabla 2-2. Puertos que deben permitir paquetes salientes provenientes de hosts de vCloud Director (continuación)

Puerto	Protocolo	Comentarios
920	TCP, UDP	rpc.statd de NFS utilizado por el servicio de transferencia.
1433	TCP	Puerto de base de datos de Microsoft SQL Server predeterminado.
5672	TCP, UDP	Opcional. Mensajes de AMQP para las extensiones de tareas.
61611	TCP	AMQP.
61616	TCP	AMQP.

- Enrute el tráfico entre los servidores de vCloud Director y los siguientes servidores a través de una red privada dedicada.
 - Servidor de la base de datos de vCloud Director
 - RabbitMQ
 - Cassandra
- Si es posible, enrute el tráfico entre los servidores de vCloud Director, vSphere y NSX a través de una red privada dedicada.
- Los switches virtuales y los switches virtuales distribuidos que admitan redes de proveedor deben estar aislados entre ellos. No pueden compartir el mismo segmento de red física de capa 2.
- Utilice NFSv4 para el almacenamiento del servicio de transferencia. La versión más común de NFS, NFSv3, no ofrece cifrado en tránsito que, en algunas configuraciones, puede permitir pruebas en ejecución o la manipulación de los datos transferidos. Las amenazas inherentes a NFSv3 se describen en el documento técnico acerca de la [seguridad de NFS en entornos de confianza y que no son de confianza](#) de SANS. Encontrará información adicional acerca de la configuración y la protección del servicio de transferencia de vCloud Director en el artículo de la base de conocimientos [2086127](#) de VMware.

Antes de instalar vCloud Director o implementar el dispositivo de vCloud Director

3

Antes de instalar vCloud Director en un servidor Linux o implementar el dispositivo de vCloud Director, es necesario preparar el entorno.

Este capítulo incluye los siguientes temas:

- [Preparar la base de datos de vCloud Director](#)
- [Preparar el almacenamiento del servidor de transferencia](#)
- [Descarga e instalación de la clave pública de VMware](#)
- [Instalar y configurar NSX Data Center for vSphere para vCloud Director](#)
- [Instalar y configurar NSX-T Data Center para vCloud Director](#)

Preparar la base de datos de vCloud Director

Las celdas de vCloud Director utilizan una base de datos para almacenar la información compartida. Antes de instalar vCloud Director en Linux, debe instalar y configurar una base de datos de vCloud Director externa. El dispositivo de vCloud Director utiliza una base de datos de PostgreSQL integrada.

Para obtener información sobre las bases de datos de vCloud Director admitidas, consulte las [matrices de interoperabilidad de productos de VMware](#).

Independientemente del software de base de datos que decida utilizar, debe crear un esquema de base de datos independiente y exclusivo para que lo utilice vCloud Director. vCloud Director no puede compartir un esquema de base de datos con ningún otro producto de VMware.

Importante vCloud Director solo admite conexiones SSL a una base de datos de PostgreSQL. Puede habilitar SSL en la base de datos de PostgreSQL durante una configuración sin supervisión de conexiones de red y base de datos, o después de crear el grupo de servidores de vCloud Director. Consulte [Referencia de configuración sin supervisión](#) y [Realizar configuraciones adicionales en la base de datos externa de PostgreSQL](#).

Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux

Las bases de datos de PostgreSQL tienen requisitos de configuración específicos cuando se utilizan con vCloud Director. Antes de instalar vCloud Director en Linux, debe instalar y configurar una instancia de base de datos y crear la cuenta de usuario de base de datos de vCloud Director.

Nota Solo vCloud Director en Linux utiliza una base de datos externa. El dispositivo de vCloud Director utiliza la base de datos de PostgreSQL integrada.

Requisitos previos

Debe estar familiarizado con los comandos, la creación de scripts y el funcionamiento de PostgreSQL.

Procedimiento

1 Configure el servidor de base de datos.

Un servidor de base de datos con 16 GB de memoria, 100 GB de almacenamiento y 4 CPU es adecuado para grupos de servidores de vCloud Director tradicionales.

2 Instale una distribución compatible de PostgreSQL en el servidor de la base de datos.

- El valor de `SERVER_ENCODING` de la base de datos debe ser UTF-8. Este valor se establece cuando se instala la base de datos y siempre coincide con la codificación que utiliza el sistema operativo de servidor de la base de datos.
- Utilice el comando `initdb` de PostgreSQL para establecer el valor de `LC_COLLATE` y `LC_CTYPE` en `en_US.UTF-8`. Por ejemplo:

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

3 Cree el usuario de la base de datos.

El usuario `vcloud` se crea con el siguiente comando.

```
create user vcloud;
```

4 Cree la instancia de la base de datos y asígnele un propietario.

Utilice un comando similar al siguiente para designar un usuario de la base de datos denominado `vcloud` como propietario de la base de datos.

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

5 Asigne una contraseña de base de datos a la cuenta del propietario de la base de datos.

El siguiente comando asigna la contraseña `vcloudpass` al propietario de la base de datos `vcloud`.

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

6 Permita que el propietario de la base de datos inicie sesión en la base de datos.

El siguiente comando asigna la opción `login` al propietario de la base de datos `vc1oud`.

```
alter role vc1oud with login;
```

Pasos siguientes

Después de crear el grupo de servidores de vCloud Director, puede configurar la base de datos de PostgreSQL para que solicite conexiones SSL desde las celdas de vCloud Director y ajuste algunos parámetros de la base de datos para obtener un rendimiento óptimo. Consulte [Realizar configuraciones adicionales en la base de datos externa de PostgreSQL](#).

Configurar una base de datos de Microsoft SQL Server externa para vCloud Director en Linux

Las bases de datos de SQL Server tienen requisitos de configuración específicos cuando se utilizan con vCloud Director. Antes de instalar vCloud Director en Linux, debe instalar y configurar una instancia de base de datos y crear la cuenta de usuario de base de datos de vCloud Director.

El rendimiento de la base de datos de vCloud Director representa un factor importante en el rendimiento y la escalabilidad globales de vCloud Director. vCloud Director utiliza el archivo `tmpdb` de SQL Server para almacenar conjuntos grandes de resultados, ordenar y administrar los datos que se leen o modifican simultáneamente. El tamaño de este archivo puede aumentar de manera significativa cuando vCloud Director sufre una fuerte carga concurrente. A modo de buena práctica, se recomienda crear el archivo `tmpdb` en un volumen independiente que tenga un rendimiento rápido de lectura y escritura. Para obtener más información acerca del rendimiento del archivo `tmpdb` y de SQL Server, consulte <http://msdn.microsoft.com/en-us/library/ms175527.aspx>.

Nota Solo vCloud Director en Linux utiliza una base de datos externa. El dispositivo de vCloud Director utiliza la base de datos de PostgreSQL integrada.

Requisitos previos

- Debe estar familiarizado con el funcionamiento, la creación de scripts y los comandos de Microsoft SQL Server.
- Para configurar Microsoft SQL Server, inicie sesión en el equipo host de SQL Server con las credenciales de administrador. Configure SQL Server para ejecutar la identidad `LOCAL_SYSTEM`, o cualquier otra identidad con privilegios para ejecutar un servicio de Windows.
- Consulte el artículo <https://kb.vmware.com/kb/2148767> de la base de conocimientos de VMware para obtener información sobre el uso de los grupos de disponibilidad AlwaysOn de Microsoft SQL Server con la base de datos de vCloud Director.

Procedimiento

1 Configure el servidor de base de datos.

Un servidor de base de datos configurado con 16 GB de memoria, 100 GB de almacenamiento y 4 CPU debería ser adecuado para la mayoría de los clústeres de servidores de vCloud Director.

2 Especifique Autenticación en modo mixto durante la configuración de SQL Server.

No se admite la Autenticación de Windows al utilizar SQL Server con vCloud Director.

3 Cree la instancia de la base de datos.

El siguiente script crea la base de datos y los archivos de registro, especificando la secuencia de intercalación adecuada.

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

Los valores que se muestran para SIZE son sugerencias. Puede que tenga que utilizar valores superiores.

4 Establezca el nivel de aislamiento de la transacción.

El siguiente script establece el nivel de aislamiento de la base de datos en READ_COMMITTED_SNAPSHOT.

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

Para obtener más información acerca del aislamiento de transacciones, consulte <http://msdn.microsoft.com/en-us/library/ms173763.aspx>.

5 Cree la cuenta de usuario de la base de datos de vCloud Director.

El siguiente script crea el nombre de usuario de la base de datos vcloud con la contraseña vcloudpass.

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
```

```
DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

- 6 Asigne los permisos a la cuenta del usuario de la base de datos de vCloud Director.

El siguiente script asigna la función db_owner al usuario de la base de datos creado en [Paso 5](#).

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

Preparar el almacenamiento del servidor de transferencia

A fin de proporcionar un almacenamiento temporal para las cargas, descargas y elementos de catálogo que se publican externamente, debe estar accesible un NFS u otro volumen de almacenamiento compartido para todos los servidores de un grupo de servidores de vCloud Director.

Importante El dispositivo de vCloud Director admite únicamente el tipo de almacenamiento compartido NFS. El proceso de implementación del dispositivo implica montar el almacenamiento del servidor de transferencia compartido NFS.

Cuando se utiliza NFS para el almacenamiento del servidor de transferencia, es necesario configurar cada celda de vCloud Director en el grupo de servidores de vCloud Director para montar y usar el almacenamiento del servidor de transferencia basado en NFS. Necesita permisos específicos de usuario y grupos para configurar cada celda con el fin de montar la ubicación basada en NFS y utilizarla como almacenamiento del servidor de transferencia.

Todos los miembros del grupo de servidores montan este volumen en el mismo punto de montaje que, por lo general, es `/opt/vmware/vcloud-director/data/transfer`. El espacio de este volumen se consume de dos formas distintas:

- Durante las transferencias, las cargas y las descargas ocupan este almacenamiento. Una vez finalizada la transferencia, se eliminan las cargas y las descargas del almacenamiento. Las transferencias que no presenten ningún progreso durante 60 minutos se considerarán como caducadas y el sistema las eliminará. Dado que las imágenes transferidas podrían ser grandes, se recomienda asignar al menos varios cientos de gigabytes a este uso.
- Este almacenamiento está ocupado por los elementos de catálogo de los catálogos que se publican externamente y para los cuales se habilita el almacenamiento en caché del contenido publicado. Los elementos de los catálogos que se publican externamente pero no habilitan el almacenamiento en caché, no ocupan este almacenamiento. Si se permite que las

organizaciones de la nube creen catálogos que se publican externamente, es de suponer que cientos o incluso miles de elementos de catálogo requieren espacio en este volumen. El tamaño de cada elemento de catálogo equivale aproximadamente al tamaño de una máquina virtual en un formato OVF comprimido.

Nota El volumen del almacenamiento del servidor de transferencia debe tener capacidad para una futura expansión.

Cómo utiliza vCloud Director los permisos del sistema de archivos en la ubicación de almacenamiento del servidor de transferencia

Para todas las celdas de vCloud Director en el grupo de servidores de vCloud Director:

- En las operaciones de nube estándar, como la carga de elementos en el catálogo, el daemon de la celda de vCloud Director escribe archivos en el almacenamiento del servidor de transferencia y los lee desde allí mediante el usuario **vcloud** en el grupo **vcloud**. El usuario **vcloud** escribe los archivos con `umask 0077`. Cuando el instalador de vCloud Director ejecuta e instala el software vCloud Director en un miembro del grupo de servidores, también crea el usuario **vcloud** y el grupo **vcloud**.
- El script `vmware-vcd-support` del recopilador de datos de registros de vCloud Director puede recopilar los registros de todas las celdas de vCloud Director en una operación y empaquetar los registros en un único archivo `tar.gz`. Cuando se ejecuta el script, escribe el archivo `tar.gz` resultante en un directorio de la ubicación de almacenamiento del servidor de transferencia mediante el identificador del usuario que invoca el script. De forma predeterminada, el único usuario que tiene permisos para ejecutar el script es el usuario **raíz**.
- El usuario **raíz** de la celda ejecuta el script que escribe el archivo `tar.gz` en el directorio `vmware-vcd-support` en la ubicación de almacenamiento del servidor de transferencia. Si desea utilizar las opciones de varias celdas para recopilar los registros de todas las celdas de una vez, el usuario **raíz** debe tener un permiso de lectura para recuperar el paquete de registros de diagnóstico de `tar.gz`.

Requisitos para configurar el servidor NFS

Existen requisitos específicos para la configuración del servidor NFS, de modo que vCloud Director pueda escribir archivos en una ubicación de almacenamiento de servidor de transferencia basada en NFS y leer archivos desde allí. Por este motivo, el usuario **vcloud** puede realizar las operaciones de nube estándar y el usuario **raíz** puede realizar una recopilación de registros de varias celdas.

- La lista de exportación del servidor NFS debe permitir el acceso de lectura y escritura a cada miembro del servidor en el grupo de servidores de vCloud Director en la ubicación compartida que se identifica en la lista de exportación. Esta capacidad permite que el usuario **vcloud** escriba y lea archivos de la ubicación compartida.

- El servidor NFS debe permitir el acceso de lectura y escritura a la ubicación compartida mediante la cuenta del sistema **raíz** en cada servidor del grupo de servidores de vCloud Director. Esta capacidad permite recopilar los registros de todas las celdas a la vez en un solo paquete mediante el script `vmware-vcd-support` con las opciones de varias celdas. A fin de cumplir este requisito, puede usar `no_root_squash` en la configuración de exportación de NFS para esta ubicación compartida.

Por ejemplo, si el servidor NFS tiene la dirección IP 192.168.120.7 y un directorio denominado `vCDspace` como espacio de transferencia para el grupo de servidores de vCloud Director con la ubicación `/nfs/vCDspace`, a fin de exportar este directorio, debe asegurarse de que la propiedad y los permisos sean **raíz:raíz** y **750**. El método para permitir el acceso de lectura y escritura a la ubicación compartida para dos celdas denominadas `vcd-cell1-IP` y `vcd-cell2-IP` es el método `no_root_squash`. Debe agregar una línea al archivo `/etc/exports`.

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

No debe haber ningún espacio entre cada dirección IP de celda y su siguiente paréntesis izquierdo inmediato en la línea de exportación. Si el servidor NFS se reinicia mientras las celdas están escribiendo datos en la ubicación compartida, el uso de la opción `sync` en la configuración de exportación impide que se dañen datos en la ubicación compartida. El uso de la opción `no_subtree_check` en la configuración de exportación mejora la confiabilidad cuando se exporta un subdirectorio de un sistema de archivos.

Cada servidor del grupo de servidores de vCloud Director debe tener permiso para montar el recurso compartido de NFS mediante la inspección de la lista de exportación para la exportación de NFS. A fin de exportar el montaje, ejecute `exportfs -a` para volver a exportar todos los recursos compartidos de NFS. Los daemons de NFS `rpcinfo -p localhost` o `service nfs status` deben estar en ejecución en el servidor.

Consideraciones al planificar la actualización de la instalación de vCloud Director a una versión posterior

Durante una actualización de un grupo de servidores de vCloud Director, se ejecuta el archivo de instalación de la versión actualizada para actualizar todos los miembros del grupo de servidores de vCloud Director. Por cuestiones de comodidad, algunas organizaciones deciden descargar el archivo de instalación para la actualización en la ubicación de almacenamiento del servidor de transferencia y ejecutarlo desde allí, ya que todas las celdas tienen acceso a esa ubicación. Debido a que debe usarse el usuario **raíz** para ejecutar el archivo de instalación de la actualización, si desea utilizar la ubicación de almacenamiento del servidor de transferencia con el fin de ejecutar una actualización, debe asegurarse de que el usuario **raíz** pueda ejecutar el archivo de instalación de la actualización cuando se esté realizando la actualización. Si no puede ejecutar la actualización como usuario **raíz**, el archivo se debe copiar en otra ubicación donde se pueda ejecutar como usuario **raíz**, por ejemplo, otro directorio fuera del montaje de NFS.

Descarga e instalación de la clave pública de VMware

El archivo de instalación se firma de manera digital. Para verificar la firma, descargue e instale la clave pública de VMware.

Utilice la herramienta `rpm` de Linux y la clave pública de VMware para verificar la firma digital del archivo de instalación de vCloud Director, o de cualquier otro archivo firmado descargado de `vmware.com`. Si instala la clave pública en el equipo en el que va a instalar vCloud Director, la verificación se realizará como parte de la instalación o actualización. También puede verificar la firma manualmente antes de iniciar la instalación o actualización. En ese caso, utilice el archivo verificado en todas las instalaciones o actualizaciones.

Nota El sitio de descarga también publica un valor de suma de comprobación para la descarga. La suma de comprobación se publica de dos formas habituales. La suma de comprobación permite verificar que los contenidos del archivo que ha descargado coinciden con los que se publicaron. No verifica la firma digital.

Procedimiento

- 1 Cree un directorio para almacenar las claves públicas de empaquetado de VMware.
- 2 Utilice un explorador web para descargar todas las claves públicas de empaquetado de VMware desde el directorio <http://packages.vmware.com/tools/keys>.
- 3 Guarde los archivos con las claves en el directorio creado.
- 4 Ejecute el siguiente comando en cada una de las claves que ha descargado para importarlas.

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

key_path es el directorio en el que ha guardado las claves.

key_name es el nombre de archivo de una clave.

Instalar y configurar NSX Data Center for vSphere para vCloud Director

Si tiene pensado que la instalación de vCloud Director utilice recursos de red de NSX Data Center for vSphere, debe instalar y configurar NSX Data Center for vSphere, y asociar una instancia única de NSX Manager con cada instancia de vCenter Server que planea incluir en la instalación de vCloud Director.

NSX Manager se incluye en la descarga de NSX Data Center for vSphere. Para obtener la información más reciente acerca de la compatibilidad entre vCloud Director y otros productos de VMware, consulte las *matrices de interoperabilidad de productos de VMware* en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Para obtener más información sobre los requisitos de red, consulte [Requisitos de configuración de red para vCloud Director](#).

Importante Este procedimiento solo se aplica cuando se lleva a cabo una nueva instalación de vCloud Director. Si está actualizando una instalación existente de vCloud Director, consulte [Capítulo 11 Actualizar vCloud Director y aplicar revisiones al dispositivo de vCloud Director](#).

Requisitos previos

Compruebe que cada uno de los sistemas vCenter Server cumpla con los requisitos previos para la instalación de NSX Manager.

Procedimiento

- 1 Realice la tarea de instalación para el dispositivo virtual de NSX Manager.
Consulte la *Guía de instalación de NSX*.
- 2 Inicie sesión en el dispositivo virtual de NSX Manager que instaló y confirme la configuración que especificó durante la instalación.
- 3 Asocie el dispositivo virtual de NSX Manager que instaló con el sistema vCenter Server que planea agregar a vCloud Director en la instalación planificada de vCloud Director.
- 4 Configure la compatibilidad VXLAN en las instancias de NSX Manager asociadas.
vCloud Director crea grupos de redes VXLAN para ofrecer recursos de red a los VDC de proveedor. Si no se ha configurado la compatibilidad VXLAN en el NSX Manager asociado, los VDCs de proveedor mostrarán un error de grupo de redes y deberá crear un grupo de otro tipo y asociarlo con el VDC de proveedor. Para obtener detalles sobre la configuración de la compatibilidad VXLAN, consulte *Guía de administración de NSX*.
- 5 (opcional) Si desea que las puertas de enlace Edge del sistema proporcionen enrutamiento distribuido, configure un clúster de NSX Controller.
Consulte la *Guía de administración de NSX*.

Instalar y configurar NSX-T Data Center para vCloud Director

Si tiene pensado que la instalación de vCloud Director utilice recursos de red de NSX-T Data Center, debe instalar y configurar NSX-T Data Center con al menos una instancia de NSX-T Manager.

NSX-T Manager se incluye en la descarga de NSX-T Data Center. Para obtener la información más reciente acerca de la compatibilidad entre vCloud Director y otros productos de VMware, consulte las *matrices de interoperabilidad de productos de VMware* en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Para obtener más información sobre los requisitos de red, consulte [Requisitos de configuración de red para vCloud Director](#).

Importante Este procedimiento solo se aplica cuando se lleva a cabo una nueva instalación de vCloud Director. Si está actualizando una instalación existente de vCloud Director, consulte [Capítulo 11 Actualizar vCloud Director y aplicar revisiones al dispositivo de vCloud Director](#).

Requisitos previos

Debe estar familiarizado con NSX-T Data Center.

Procedimiento

- 1** Instale el dispositivo virtual de NSX-T Manager.
Consulte la *Guía de instalación de NSX-T*.
- 2** Prepare los hosts de ESXi con los que desee trabajar con NSX-T Data Center.
Consulte la *Guía de instalación de NSX-T*.
- 3** Cree nodos de transporte y zonas de transporte para sus requisitos de nube.
Consulte la *Guía de instalación de NSX-T*.
- 4** Configure los clústeres y los nodos de Edge.
Consulte la *Guía de instalación de NSX-T*.
- 5** Configure los enrutadores de nivel 0 y nivel 1.
Consulte la *Guía de administración de NSX-T*.
- 6** Configure una o varias VLAN o superponga los conmutadores lógicos que desee importar a la instalación de vCloud Director.
Consulte la *Guía de administración de NSX-T*.

Pasos siguientes

Después de instalar vCloud Director, puede registrar la instancia de NSX-T Manager en su nube. Para obtener información sobre el registro de una instancia de NSX-T Manager, consulte la *Guía de programación de vCloud API para proveedores de servicios*.

Creación y administración de certificados SSL para vCloud Director en Linux

4

vCloud Director usa SSL para proteger la comunicación entre clientes y servidores. Cada servidor de vCloud Director debe admitir dos endpoints de SSL diferentes: uno para HTTPS y otro para las comunicaciones de proxy de consola.

Los endpoints pueden ser direcciones IP independientes o una sola dirección IP con dos puertos diferentes. Cada extremo requiere su propio certificado SSL. Puede usar el mismo certificado para ambos endpoints, por ejemplo, si utiliza un certificado comodín.

Este capítulo incluye los siguientes temas:

- [Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux](#)
- [Crear certificados SSL autofirmados para vCloud Director en Linux](#)
- [Crear un almacén de claves de certificados SSL firmados por una entidad de certificación para vCloud Director en Linux](#)
- [Crear un almacén de claves de certificados SSL firmados por una entidad de certificación con claves privadas importadas para vCloud Director en Linux](#)

Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux

Al instalar vCloud Director para Linux, debe crear dos certificados para cada miembro del grupo de servidores e importar los certificados en los almacenes de claves del host.

Nota Antes de crear los certificados para los miembros del grupo de servidores, debe instalar vCloud Director en Linux. El dispositivo de vCloud Director crea certificados SSL autofirmados durante el primer arranque.

Procedimiento

- 1 Inicie sesión en el servidor de vCloud Director como **raíz**.
- 2 Enumere las direcciones IP del servidor.

Utilice un comando (como `ifconfig`) para detectar las direcciones IP de este servidor.

- 3 Ejecute el comando siguiente con cada una de las direcciones IP para recuperar el FQDN al que están enlazadas.

```
nslookup ip-address
```

- 4 Anote todas las direcciones IP y sus FQDN asociados. Si no utiliza la misma dirección IP para los servicios HTTPS y de proxy de consola, decida qué dirección se debe usar con cada servicio.

Es necesario proporcionar los FQDN cuando se crean los certificados y las direcciones IP durante la configuración de las conexiones de red y base de datos. Anote el resto de los FQDN que pueden alcanzar la dirección IP porque debe proporcionarlos si desea que el certificado incluya un nombre alternativo del firmante.

Pasos siguientes

Cree los certificados para los dos endpoints. Puede utilizar certificados firmados por una entidad de certificación de confianza o autofirmados.

Nota Los certificados firmados por una entidad de certificación ofrecen el nivel más alto de confianza.

- Para obtener información sobre cómo crear e importar certificados SSL firmados por una entidad de certificación, consulte [Crear un almacén de claves de certificados SSL firmados por una entidad de certificación para vCloud Director en Linux](#).
- Para obtener información sobre cómo crear certificados SSL autofirmados, consulte [Crear certificados SSL autofirmados para vCloud Director en Linux](#).
- Para obtener información sobre cómo importar sus propios archivos de clave privada y de certificado firmado por una entidad de certificación, consulte [Crear un almacén de claves de certificados SSL firmados por una entidad de certificación con claves privadas importadas para vCloud Director en Linux](#).

Crear certificados SSL autofirmados para vCloud Director en Linux

Los certificados de firma automática ofrecen una manera cómoda de configurar SSL para vCloud Director en entornos donde exista mínima preocupación por la confianza.

Cada servidor de vCloud Director requiere dos certificados SSL en un archivo de almacén de claves JCEKS: uno para el servicio HTTPS y otro para el de proxy de consola.

Se utiliza `cell-management-tool` para crear los certificados SSL autofirmados. La utilidad `cell-management-tool` se instala en la celda antes de que se ejecute el agente de configuración y después de que se ejecute el archivo de instalación. Consulte la [Instalar vCloud Director en el primer miembro de un grupo de servidores](#).

Importante En estos ejemplos se especifica un tamaño de clave de 2048 bits, pero conviene evaluar los requisitos de seguridad de la instalación antes de elegir un tamaño adecuado de clave. Los tamaños de clave inferiores a 1024 bits ya no se admiten según la publicación especial NIST 800-131A.

Procedimiento

- 1 Inicie sesión directamente o mediante un cliente SSH en el sistema operativo del servidor de vCloud Director como usuario **raíz**.
- 2 Ejecute el comando para crear un par de claves pública y privada para los servicios HTTPS y de proxy de consola.

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

El comando crea o actualiza un almacén de claves en `certificates.ks` con la contraseña `passwd`. `cell-management-tool` crea los certificados utilizando los valores predeterminados del comando. Según la configuración de DNS del entorno, el CN del emisor se establece en la dirección IP o el FQDN de cada servicio. El certificado utiliza la longitud de clave predeterminada de 2048 bits y caduca un año después de su creación.

Importante El archivo de almacén de claves y el directorio en el que se almacena deben ser legibles para el usuario **vcloud.vcloud**. El instalador de vCloud Director crea este usuario y grupo.

Pasos siguientes

Anote el nombre de la ruta de acceso al almacén de claves. El nombre de la ruta de acceso al almacén de claves se precisa al ejecutar el script de configuración para crear las conexiones de red y de base de datos de la celda de vCloud Director. Consulte [Configuración de conexiones de red y de base de datos](#).

Crear un almacén de claves de certificados SSL firmados por una entidad de certificación para vCloud Director en Linux

La creación y la importación de certificados firmados por una entidad de certificación proporcionan el nivel más alto de confianza para las comunicaciones de SSL y ayudan a proteger las conexiones dentro de la infraestructura de nube.

Cada servidor de vCloud Director requiere dos certificados SSL para proteger las comunicaciones entre los clientes y los servidores. Cada servidor de vCloud Director debe admitir dos endpoints de SSL diferentes: uno para HTTPS y otro para las comunicaciones de proxy de consola.

Los dos endpoints pueden ser direcciones IP independientes o una sola dirección IP con dos puertos diferentes. Cada extremo requiere su propio certificado SSL. Puede usar el mismo certificado para ambos endpoints, por ejemplo, si utiliza un certificado comodín.

Los certificados de ambos endpoints deben incluir un nombre distintivo X.500 y una extensión de nombre alternativo del firmante X.509.

Puede utilizar certificados firmados por una entidad de certificación de confianza o autofirmados.

Se utiliza `cell-management-tool` para crear los certificados SSL autofirmados. La utilidad `cell-management-tool` se instala en la celda antes de que se ejecute el agente de configuración y después de que se ejecute el archivo de instalación. Consulte la [Instalar vCloud Director en el primer miembro de un grupo de servidores](#).

Si ya cuenta con sus propios archivos de clave privada y de certificado firmado por una entidad de certificación, siga el procedimiento que se describe en [Crear un almacén de claves de certificados SSL firmados por una entidad de certificación con claves privadas importadas para vCloud Director en Linux](#).

Importante En estos ejemplos se especifica un tamaño de clave de 2048 bits, pero conviene evaluar los requisitos de seguridad de la instalación antes de elegir un tamaño adecuado de clave. Los tamaños de clave inferiores a 1024 bits ya no se admiten según la publicación especial NIST 800-131A.

Requisitos previos

- Verifique que puede acceder a un equipo con Java Runtime Environment 8 o una versión posterior, de manera que pueda utilizar el comando `keytool` para importar los certificados. El instalador de vCloud Director coloca una copia de `keytool` en `/opt/vmware/vcloud-director/jre/bin/keytool`. No obstante, puede realizar este procedimiento en cualquier equipo en el que se haya instalado Java Runtime Environment. Los certificados que hayan sido creados con el comando `keytool` desde cualquier otra fuente no se admiten en vCloud Director. Estos ejemplos de línea de comandos dan por sentado que `keytool` se encuentra en la ruta del usuario.
- Familiarícese con el comando `keytool`.
- Para obtener más información sobre las opciones disponibles para el comando `generate-certs`, consulte [Generar certificados autofirmados para los endpoints de proxy de consola y HTTPS](#).
- Para obtener más información sobre las opciones disponibles para el comando `certificates`, consulte [Sustituir certificados para los endpoints de proxy de consola y HTTP](#).

Procedimiento

- 1 Inicie sesión directamente o mediante un cliente SSH en el SO de la celda del servidor de vCloud Director como **raíz**.
- 2 Ejecute el comando para crear un par de claves pública y privada para los servicios HTTPS y de proxy de consola.

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

El comando crea o actualiza un almacén de claves en `certificates.ks` con la contraseña especificada. Los certificados se crean utilizando los valores predeterminados del comando. Según la configuración de DNS del entorno, el CN del emisor se establece en la dirección IP o el FQDN de cada servicio. El certificado utiliza la longitud de clave predeterminada de 2048 bits y caduca un año después de su creación.

Importante El archivo de almacén de claves y el directorio en el que se almacena deben ser legibles para el usuario **vcloud.vcloud**. El instalador de vCloud Director crea este usuario y grupo.

- 3 Cree una solicitud de firma del certificado para los servicios HTTPS y de proxy de consola.

Importante Si utiliza direcciones IP independientes para los servicios HTTPS y de proxy de consola, ajuste los nombres de host y las direcciones IP en los comandos que se indican a continuación.

- a Cree una solicitud de firma del certificado en el archivo `http.csr`.

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

- b Cree una solicitud de firma del certificado en el archivo `consoleproxy.csr`.

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

- 4 Envíe las solicitudes de firma del certificado a la entidad de certificación.

Si la autoridad de certificación le exige especificar un tipo de servidor web, utilice Jakarta Tomcat.

Obtiene los certificados firmados por una entidad de certificación.

5 Importe los certificados firmados al almacén de claves JCEKS.

- a Importe el certificado raíz de la entidad de certificación del archivo `root.cer` al archivo de almacén de claves `certificates.ks`.

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

- b Si ha recibido certificados intermedios, impórtelos del archivo `intermediate.cer` al archivo de almacén de claves `certificates.ks`.

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

- c Importe el certificado del servicio HTTPS.

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

- d Importe el certificado del servicio de proxy de consola.

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

Los comandos sobrescriben el archivo `certificates.ks` con las versiones de los certificados firmadas por entidades de certificación recientemente adquiridas.

- 6 Para comprobar si los certificados se han importado en el almacén de claves JCEKS, ejecute el comando para que aparezca el contenido del archivo del almacén.

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

- 7 Repita este procedimiento para todos los servidores vCloud Director del grupo de servidores.

Pasos siguientes

- Si aún no ha configurado la instancia de vCloud Director, ejecute el script `configure` para importar el almacén de claves de certificados en vCloud Director. Consulte [Configuración de conexiones de red y de base de datos](#).

Nota Si creó el archivo de almacén de claves `certificates.ks` en un equipo que no sea el servidor en el cual haya generado la lista de nombres de dominio totalmente cualificados y sus direcciones IP, copie dicho archivo en ese servidor ahora. Necesita el nombre de la ruta de acceso al almacén de claves cuando ejecute el script de configuración.

- Si ya ha instalado y configurado la instancia de vCloud Director, utilice el comando `certificates` de la herramienta de administración de celdas para importar el almacén de claves de certificados. Consulte [Sustituir certificados para los endpoints de proxy de consola y HTTP](#).

Crear un almacén de claves de certificados SSL firmados por una entidad de certificación con claves privadas importadas para vCloud Director en Linux

Si cuenta con sus propios archivos de clave privada y de certificado firmado por una entidad de certificación, antes de importar los almacenes de claves en el entorno de vCloud Director, cree archivos de almacén de claves en los que importar los certificados y las claves privadas de los servicios HTTPS y de proxy de consola.

Requisitos previos

- Consulte la [Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux](#).
- Verifique que puede acceder a un equipo con Java Runtime Environment 8 o una versión posterior, de manera que pueda utilizar el comando `keytool` para importar los certificados. El instalador de vCloud Director coloca una copia de `keytool` en `/opt/vmware/vcloud-director/jre/bin/keytool`. No obstante, puede realizar este procedimiento en cualquier equipo en el que se haya instalado Java Runtime Environment. Los certificados que hayan sido creados con el comando `keytool` desde cualquier otra fuente no se admiten en vCloud Director. Estos ejemplos de línea de comandos dan por sentado que `keytool` se encuentra en la ruta del usuario.
- Familiarícese con el comando `keytool`.
- Descargue e instale OpenSSL.
- Para obtener más información sobre las opciones disponibles para el comando `certificates`, consulte [Sustituir certificados para los endpoints de proxy de consola y HTTP](#).

Procedimiento

- 1 Si dispone de certificados intermedios, ejecute el comando para combinarlos con el certificado raíz firmado por una entidad de certificación y crear una cadena de certificados.

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

- 2 Con la ayuda de OpenSSL, cree archivos de almacén de claves PKCS12 intermedios para los servicios HTTPS y de proxy de consola, con la clave privada, la cadena de certificados y el alias correspondiente. Especifique una contraseña para cada archivo de almacén de claves.

- a Cree el archivo de almacén de claves para el servicio HTTPS.

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

- b Cree el archivo de almacén de claves para el servicio de proxy de consola.

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

- 3 Utilice keytool para importar los almacenes de claves PKCS12 al almacén de claves JCEKS.

- a Ejecute el comando para importar el almacén de claves PKCS12 para el servicio HTTPS.

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

- b Ejecute el comando para importar el almacén de claves PKCS12 para el servicio de proxy de consola.

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

- 4 Para comprobar si los certificados se han importado en el almacén de claves JCEKS, ejecute el comando para que aparezca el contenido del archivo del almacén.

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

- 5 Repita este procedimiento en todas las celdas de vCloud Director del entorno.

Pasos siguientes

- Si aún no ha configurado la instancia de vCloud Director, ejecute el script configure para importar el almacén de claves de certificados en vCloud Director. Consulte [Configuración de conexiones de red y de base de datos](#).

Nota Si creó el archivo de almacén de claves `certificates.ks` en un equipo distinto del servidor donde generó la lista de nombres de dominio completos y sus direcciones IP asociadas, copie dicho archivo en ese servidor. Necesita el nombre de la ruta de acceso al almacén de claves cuando ejecute el script de configuración.

- Si ya ha instalado y configurado la instancia de vCloud Director, utilice el comando `certificates` de la herramienta de administración de celdas para importar el almacén de claves de certificados. Consulte [Sustituir certificados para los endpoints de proxy de consola y HTTP](#).

Instalar vCloud Director en Linux

5

Es posible crear un grupo de servidores de vCloud Director al instalar el software de vCloud Director de uno o varios servidores Linux. La instalación y configuración del primer miembro del grupo crea un archivo de respuesta que debe utilizar para configurar miembros adicionales del grupo.

Este procedimiento se aplica solo a las instalaciones nuevas. Si planea actualizar una instalación existente de vCloud Director, consulte [Capítulo 11 Actualizar vCloud Director y aplicar revisiones al dispositivo de vCloud Director](#).

Importante No se admiten instalaciones mixtas de vCloud Director en implementaciones de Linux y dispositivos de vCloud Director en un grupo de servidores.

Requisitos previos

- Compruebe que los servidores de destino para el grupo de servidores cumplan con [Capítulo 2 Requisitos de hardware y de software de vCloud Director](#).
- Compruebe que se haya creado un certificado SSL para cada endpoint de los servidores de destino en el grupo de servidores. Todos los usuarios deben poder leer todos los directorios en el nombre de ruta a los certificados SSL. El uso de la misma ruta de almacén de claves en todos los miembros de un grupo de servidores simplifica el proceso de instalación, por ejemplo, /tmp/certificates.ks. Consulte [Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux](#).
- Compruebe que se haya preparado un NFS u otro volumen de almacenamiento compartido que sea accesible para todos los servidores de destino en el grupo de servidores de vCloud Director. Consulte [Preparar el almacenamiento del servidor de transferencia](#).
- Compruebe que se haya creado una base de datos de vCloud Director que sea accesible para todos los servidores del grupo. Consulte [Preparar la base de datos de vCloud Director](#). Compruebe que se inicie el servicio de base de datos cuando se reinicia el servidor de base de datos.
- Compruebe que todos los servidores de vCloud Director, el servidor de base de datos, todos los sistemas de vCenter Server y las instancias de NSX Manager asociadas puedan resolver cada nombre de host en el entorno como se describe en [Requisitos de configuración de red para vCloud Director](#).

- Verifique que todos los vCloud Director Servers y el servidor de base de datos estén sincronizados con un servidor horario de la red con las tolerancias mencionadas en [Requisitos de configuración de red para vCloud Director](#).
- Si planea importar usuarios o grupos a partir de un servicio LDAP, verifique que el servicio sea accesible para cada vCloud Director Server.
- Abra los puertos de firewall, tal como se ilustra en [Requisitos de seguridad de red](#). El puerto 443 debe estar abierto entre vCloud Director y los sistemas vCenter Server.

Procedimiento

1 [Instalar vCloud Director en el primer miembro de un grupo de servidores](#)

Después de preparar el entorno y comprobar los requisitos previos, puede empezar a crear el grupo de servidores de vCloud Director mediante la ejecución del instalador de vCloud Director en el primer servidor de destino de Linux.

2 [Configuración de conexiones de red y de base de datos](#)

Después de instalar vCloud Director en el primer miembro del grupo de servidores, debe ejecutar el script de configuración que crea las conexiones de red y de base de datos de esta celda. El script crea un archivo de respuesta que deberá utilizar al configurar los miembros adicionales del grupo de servidores.

3 [Instalar vCloud Director en un miembro adicional de un grupo de servidores](#)

Puede agregar servidores a un grupo de servidores de vCloud Director en cualquier momento. Dado que todos los servidores de un grupo de servidores deben configurarse con los mismos detalles de conexión de base de datos, es necesario utilizar el archivo de respuesta que se creó al configurar el primer miembro del grupo.

4 [Configurar vCloud Director](#)

Después de instalar y configurar todos los servidores en el grupo de servidores de vCloud Director, debe configurar su instalación de vCloud Director. El programa de instalación de vCloud Director inicializa la base de datos de vCloud Director con una clave de licencia, la cuenta de administrador del sistema y la información relacionada.

Pasos siguientes

Puede empezar a agregar recursos a la instalación de vCloud Director. Para comenzar a usar vCloud Director, consulte *Guía del administrador de vCloud Director*.

Instalar vCloud Director en el primer miembro de un grupo de servidores

Después de preparar el entorno y comprobar los requisitos previos, puede empezar a crear el grupo de servidores de vCloud Director mediante la ejecución del instalador de vCloud Director en el primer servidor de destino de Linux.

vCloud Director para Linux se distribuye como archivo ejecutable firmado digitalmente con un nombre con el formato `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, donde *v.v.v* representa la versión de producto y *nnnnnn*, el número de compilación. Por ejemplo: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Con este ejecutable, se instala o actualiza vCloud Director.

El instalador de vCloud Director verifica que el servidor de destino cumpla todos los requisitos previos de plataforma e instala el software de vCloud Director en él.

Requisitos previos

- Verifique que dispone de credenciales de superusuario en el servidor de destino.
- Si desea que el instalador verifique la firma digital del archivo de instalación, descargue e instale la clave pública de VMware en el servidor de destino. Si ya ha verificado la firma digital del archivo de instalación, no es necesario volver a verificarla durante la instalación. Consulte [Descarga e instalación de la clave pública de VMware](#).

Procedimiento

- 1 Inicie sesión en el servidor de destino como **raíz**.

- 2 Descargue el archivo de instalación en el servidor de destino.

Si ha comprado el software en un medio, copie el archivo de instalación en una ubicación que sea accesible para el servidor de destino.

- 3 Verifique que la suma de comprobación de la descarga coincida con la publicada en la página de descargas.

Los valores de las sumas de comprobación MD5 y SHA1 se publican en la página de descargas. Utilice la herramienta adecuada para verificar que la suma de comprobación del archivo de instalación descargado coincida con la que se muestra en la página de descargas. Un comando de Linux con la forma siguiente muestra la suma de comprobación para *installation-file*.

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

El comando devuelve la suma de comprobación del archivo de instalación que debe coincidir con la suma de comprobación MD5 de la página de descargas.

- 4 Asegúrese de que se pueda ejecutar el archivo de instalación.

El archivo de instalación requiere permiso de ejecución. Para asegurarse de que dispone de dicho permiso, abra una ventana de consola, shell o terminal, y ejecute el siguiente comando Linux, donde *archivo-de-instalación* es el nombre de ruta completo del archivo de instalación de vCloud Director.

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

5 Ejecute el archivo de instalación.

Para ejecutar el archivo de instalación, introduzca el nombre de ruta completo; por ejemplo:

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

El archivo incluye un script de instalación y un paquete RPM integrado.

Nota No se puede ejecutar el archivo de instalación desde un directorio cuya ruta de acceso incluya espacios integrados.

Si no instaló la clave pública de VMware en el servidor de destino, el instalador imprime una advertencia con el siguiente formato:

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

El instalador realiza las siguientes acciones.

- a Comprueba que el host cumpla con todos los requisitos.
- b Verifica la firma digital del archivo de instalación.
- c Crea el usuario y el grupo vcloud.
- d Desempaqueta el paquete RPM de vCloud Director.
- e Instala el software.

Después de completar la instalación, el instalador le indicará que ejecute el script de configuración para configurar las conexiones de red y de base de datos.

6 Seleccione si desea ejecutar el script de configuración.

- a Para ejecutar el script de configuración en un modo interactivo, introduzca **y** y presione Intro.
- b Para ejecutar el script de configuración más adelante en un modo interactivo o sin supervisión, introduzca **n** y presione Intro.

Configuración de conexiones de red y de base de datos

Después de instalar vCloud Director en el primer miembro del grupo de servidores, debe ejecutar el script de configuración que crea las conexiones de red y de base de datos de esta celda. El script crea un archivo de respuesta que deberá utilizar al configurar los miembros adicionales del grupo de servidores.

Todos los miembros del grupo de servidores de vCloud Director comparten la conexión de base de datos y otros detalles de configuración. Al ejecutar el script de configuración en el primer miembro del grupo de servidores de vCloud Director, el script crea un archivo de respuesta que conserva la información de las conexiones de base de datos para su uso en las instalaciones de servidor subsiguientes.

Puede ejecutar el script de configuración en modo interactivo y en modo sin supervisión. Para una configuración interactiva, ejecute el comando sin opciones; el script solicitará la información de configuración necesaria. Para una configuración sin supervisión, proporcione la información de configuración mediante las opciones del comando.

Si desea utilizar una sola dirección IP con dos puertos diferentes para el servicio HTTP y el servicio de proxy de la consola, debe ejecutar el script de configuración en el modo sin supervisión.

Nota La herramienta de administración de celdas incluye subcomandos que se pueden utilizar para cambiar los detalles de conexiones de red y de base de datos configurados inicialmente. Los cambios realizados mediante estos subcomandos se escriben en el archivo de configuración global y en el archivo de respuesta. Para obtener información sobre el uso de la herramienta de administración de celdas, consulte *Guía del administrador de vCloud Director*.

Requisitos previos

- Para una configuración interactiva, revise [Referencia de configuración interactiva](#).
- Para una configuración sin supervisión, revise [Referencia de configuración sin supervisión](#).
- Para una configuración sin supervisión, compruebe que el valor de la variable del entorno VCLLOUD_HOME esté configurado como el nombre completo de la ruta de acceso del directorio en el que está instalado vCloud Director. Generalmente, este valor es /opt/vmware/vcloud-director.

Procedimiento

1 Inicie sesión en el servidor de vCloud Director como raíz.

2 Ejecute el comando configure:

- Para el modo interactivo, ejecute el comando y, en los mensajes, proporcione la información necesaria.

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

- Para el modo sin supervisión, ejecute el comando con las opciones y los argumentos adecuados.

```
/opt/vmware/vcloud-director/bin/configureoptions -unattended
```

El script valida la información. A continuación:

- a Inicializa la base de datos y la conecta con el servidor.
- b Muestra una dirección URL a la que se puede conectar el asistente para la **instalación de VMware vCloud Director** después de que se inicia el servicio vCloud Director.
- c Ofrece la posibilidad de iniciar la celda de vCloud Director.

- 3 (opcional) Tome nota de la URL del asistente para la **instalación de VMware vCloud Director** y escriba **y** para iniciar el servicio de vCloud Director.

Para iniciar el servicio en otro momento, puede ejecutar el comando `service vmware-vcd start`.

Resultados

La información de conexión de base de datos y otros datos reutilizables que haya proporcionado durante la configuración se conservan en un archivo de respuesta que se encuentra en `/opt/vmware/vcloud-director/etc/responses.properties` en este servidor. Este archivo contiene información confidencial que debe volver a utilizar al agregar más servidores al grupo de servidores.

Pasos siguientes

Guarde una copia del archivo de respuesta en un lugar seguro. Restrinja el acceso al mismo y asegúrese de tener una copia de seguridad en un lugar seguro. Al crear la copia de seguridad del archivo, evite enviar textos no cifrados a través de redes públicas.

Si tiene pensado agregar servidores al grupo de servidores, monte el almacenamiento de transferencia compartido en `/opt/vmware/vcloud-director/data/transfer`.

Referencia de configuración interactiva

Al ejecutar el script `configure` en un modo interactivo, el script solicitará la siguiente información.

Para aceptar un valor predeterminado, presione Intro.

Tabla 5-1. Información necesaria durante una configuración interactiva de red y base de datos

Información necesaria	Descripción
Dirección IP del servicio HTTP	El valor predeterminado es la primera dirección IP disponible.
Dirección IP del servicio de proxy de la consola	El valor predeterminado es la primera dirección IP disponible. Nota Si desea utilizar una sola dirección IP con dos puertos diferentes para el servicio HTTP y el servicio de proxy de la consola, debe ejecutar el script de configuración en el modo sin supervisión.
Ruta completa al archivo del almacén de claves de Java	Por ejemplo, <code>/opt/keystore/certificates.ks</code> .
Contraseña del almacén de claves	Consulte Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux .
Contraseña de clave privada del certificado SSL de HTTP	Consulte Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux .
Contraseña de clave privada del certificado de SSL de proxy de la consola	Consulte Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux .

Tabla 5-1. Información necesaria durante una configuración interactiva de red y base de datos (continuación)

Información necesaria	Descripción
Habilitar el registro de auditoría remoto a un host de syslog	<p>Los servicios de cada celda de vCloud Director registran los mensajes de auditoría en la base de datos de vCloud Director, donde se conservan por 90 días. Para conservar los mensajes de auditoría durante más tiempo, puede configurar los servicios de vCloud Director para que envíen mensajes de auditoría a la utilidad syslog además de a la base de datos de vCloud Director.</p> <ul style="list-style-type: none"> ■ Para omitir, presione Intro. ■ Para habilitar, introduzca la dirección IP o el nombre del host de syslog.
Si se habilitó el registro de auditoría remoto, el puerto UDP del host de syslog	El valor predeterminado es 514.
Tipo de base de datos	<p>PostgreSQL o Microsoft SQL Server.</p> <p>El valor predeterminado es PostgreSQL.</p>
Nombre de host o dirección IP del servidor de base de datos	El servidor en el que se ejecuta la base de datos.
Puerto de base de datos	<p>Para PostgreSQL, el valor predeterminado es 5432.</p> <p>Para Microsoft SQL Server, el valor predeterminado es 1433.</p>
Nombre de la base de datos	El valor predeterminado es vcloud.
Si el tipo de base de datos es Microsoft SQL Server, la instancia de la base de datos	El valor predeterminado es la instancia predeterminada.
Nombre de usuario de la base de datos	Consulte Preparar la base de datos de vCloud Director .
Contraseña de la base de datos	Consulte Preparar la base de datos de vCloud Director .
Unirse o no al programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de VMware	<p>Este producto forma parte del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware. En el Centro de Seguridad y Confianza, en http://www.vmware.com/trustvmware/ceip.html, hay información acerca de los datos recopilados a través del CEIP y los fines para los cuales VMware los utiliza. En cualquier momento, puede usar la herramienta de administración de celdas para unirse o abandonar el CEIP de VMware para este producto. Consulte la referencia a la herramienta de administración de celdas en la <i>Guía del administrador de vCloud Director</i>.</p> <p>Para unirse al programa, introduzca y.</p> <p>Si prefiere no unirse al programa CEIP de VMware, introduzca n.</p>

Referencia de configuración sin supervisión

Al ejecutar el script `configure` en el modo sin supervisión, debe proporcionar la información de configuración en la línea de comandos como argumentos y opciones.

Tabla 5-2. Argumentos y opciones de la utilidad de configuración

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Muestra un resumen de los argumentos y las opciones de configuración.
<code>--config-file (-c)</code>	Ruta de acceso al archivo <code>global.properties</code>	La información que proporciona cuando ejecuta la utilidad de configuración se guarda en este archivo. Si omite esta opción, la ubicación predeterminada es <code>/opt/vmware/vcloud-director/etc/global.properties</code> .
<code>--console-proxy-ip (-cons)</code>	Dirección IPv4, con número de puerto opcional	El sistema usa esta dirección para el servicio de proxy de la consola de vCloud Director. Por ejemplo, <code>10.17.118.159</code> .
<code>--console-proxy-port-https</code>	Entero dentro del rango 0-65535	Número de puerto que debe usarse para el servicio de proxy de la consola de vCloud Director.
<code>--database-ssl</code>	<code>true</code> o <code>false</code>	Si utiliza una base de datos de PostgreSQL, puede configurar la base de datos para que solicite una conexión SSL firmada correctamente desde vCloud Director. Se omite si <code>--database-type</code> no es <code>postgres</code> . Si desea configurar la base de datos de PostgreSQL para que use un certificado autofirmado o privado, consulte Realizar configuraciones adicionales en la base de datos externa de PostgreSQL .
<code>--database-host (-dbhost)</code>	Dirección IP o nombre de dominio completo del host de base de datos de vCloud Director	Consulte Preparar la base de datos de vCloud Director .
<code>--database-domain (-dbdomain)</code>	Dominio de usuario de la base de datos SQL Server	Es opcional si <code>--database-type</code> es <code>sqlserver</code> .
<code>--database-instance (-dbinstance)</code>	Instancia de base de datos SQL Server	Se usa si <code>--database-type</code> es <code>sqlserver</code> .

Tabla 5-2. Argumentos y opciones de la utilidad de configuración (continuación)

Opción	Argumento	Descripción
--database-name (-dbname)	Nombre del servicio de base de datos	Consulte Preparar la base de datos de vCloud Director .
--database-password (-dbpassword)	Contraseña para el usuario de la base de datos. Puede ser un valor nulo.	Consulte Preparar la base de datos de vCloud Director .
--database-port (-dbport)	Número de puerto usado por el servicio de base de datos en el host de base de datos	Consulte Preparar la base de datos de vCloud Director .
--database-type (-dbtype)	Tipo de la base de datos. Puede ser: <ul style="list-style-type: none"> ■ postgres ■ sqlserver 	Consulte Preparar la base de datos de vCloud Director .
--database-user (-dbuser)	Nombre de usuario del usuario de la base de datos	Consulte Preparar la base de datos de vCloud Director .
--enable-ceip	true o false	Este producto forma parte del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware. En el Centro de Seguridad y Confianza, en http://www.vmware.com/trustvmware/ceip.html , hay información acerca de los datos recopilados a través del CEIP y los fines para los cuales VMware los utiliza. En cualquier momento, puede usar la herramienta de administración de celdas para unirse o abandonar el CEIP de VMware para este producto. Consulte la referencia a la herramienta de administración de celdas en la <i>Guía del administrador de vCloud Director</i> .
--uuid (-g)	Ninguno	Genera un nuevo identificador único para la celda.
--primary-ip (-ip)	Dirección IPv4, con número de puerto opcional	El sistema usa esta dirección para el servicio de la interfaz web de vCloud Director. Por ejemplo, <i>10.17.118.159</i> .
--primary-port-http	Entero en el rango de 0 a 65535	Número de puerto que ha de usarse para las conexiones HTTP (inseguras) con el servicio de la interfaz web de vCloud Director

Tabla 5-2. Argumentos y opciones de la utilidad de configuración (continuación)

Opción	Argumento	Descripción
--primary-port-https	Entero dentro del rango 0-65535	Número de puerto que debe usarse para las conexiones HTTPS (inseguras) con el servicio de la interfaz web de vCloud Director
--keystore (-k)	Ruta de acceso al almacén de claves de Java que contiene sus certificados SSL y claves privadas	Debe ser un nombre completo de la ruta de acceso. Por ejemplo, /opt/keystore/certificates.ks.
--syslog-host (-loghost)	Dirección IP o nombre de dominio completo del host del servidor Syslog	Los servicios de cada celda de vCloud Director registran los mensajes de auditoría en la base de datos de vCloud Director, donde se conservan por 90 días. Para conservar los mensajes de auditoría durante más tiempo, puede configurar los servicios de vCloud Director para que envíen mensajes de auditoría a la utilidad syslog además de a la base de datos de vCloud Director.
--syslog-port (-logport)	Entero dentro del rango 0-65535	El puerto en el cual el proceso syslog supervisa el servidor especificado. El valor predeterminado es 514 si no se ha especificado.
--response-file (-r)	Ruta de acceso al archivo de respuesta	<p>Debe ser un nombre completo de la ruta de acceso. El valor predeterminado es /opt/vmware/vcloud-director/etc/responses.properties si no se ha especificado. Toda la información que proporciona al ejecutar configure se conserva en este archivo.</p> <p>Importante Este archivo contiene información confidencial que debe volver a utilizar al agregar más servidores al grupo de servidores. Conserve el archivo en un lugar seguro y ponerlo a disposición solamente cuando sea necesario.</p>
--unattended-installation (-unattended)	Ninguno	Especifica la instalación sin supervisión.
--keystore-password (-w)	Contraseña del almacén de claves de certificados SSL	Contraseña del almacén de claves de certificados SSL.

Ejemplo: Configuración sin supervisión con dos direcciones IP

El siguiente comando de ejemplo ejecuta una configuración sin supervisión de un servidor vCloud Director con dos direcciones IP diferentes para el servicio HTTP y el servicio de proxy de la consola.

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

Ejemplo: Configuración sin supervisión con una sola dirección IP

El siguiente comando de ejemplo ejecuta una configuración sin supervisión de un servidor de vCloud Director con una sola dirección IP y dos puertos diferentes para el servicio HTTP y el servicio de proxy de la consola.

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

Proteger y reutilizar el archivo de respuesta

Los detalles de conexión de red y de base de datos que configura en la primera celda de vCloud Director se guardan en un archivo de respuesta. Este archivo contiene información confidencial que debe volver a utilizar al agregar más servidores al grupo de servidores. Debe conservar el archivo en una ubicación segura.

El archivo de respuesta se crea en `/opt/vmware/vcloud-director/etc/responses.properties` en el primer servidor para el cual configure las conexiones de red y de base de datos. Cuando agregue servidores al grupo, debe utilizar una copia del archivo de respuesta para proporcionar los parámetros de configuración que comparten todos los servidores.

Importante La herramienta de administración de celdas incluye subcomandos que se pueden utilizar para cambiar los detalles de conexiones de red y de base de datos especificados inicialmente. Los cambios que realice usando estas herramientas se escriben en el archivo de configuración global y el archivo de respuesta, por lo que debe estar seguro de tener listo el archivo de respuesta (en `/opt/vmware/vcloud-director/etc/responses.properties`) y que pueda escribirse en él antes de usar cualquiera de los comandos que pueden modificarlo.

Procedimiento

1 Proteja el archivo de respuesta.

Guarde una copia del archivo en una ubicación segura. Restrinja el acceso al mismo y asegúrese de tener una copia de seguridad en un lugar seguro. Al crear la copia de seguridad del archivo, evite enviar texto no cifrado a través de redes públicas.

2 Vuelva a utilizar el archivo de respuesta.

- a Copie el archivo en un lugar donde sea accesible para el servidor que vaya a configurar.

Nota Debe instalar el software de vCloud Director en un servidor para poder utilizar de nuevo el archivo de respuesta para configurarlo. El usuario `vcloud.vcloud` debe poder leer todos los directorios en la ruta al archivo de respuesta, como se muestra en este ejemplo.

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

El instalador crea este usuario y grupo.

- b Ejecute el script de configuración utilizando la opción `-r` y especificando el nombre de ruta al archivo de respuesta.

Inicie sesión como usuario `root`, abra una ventana de terminal, shell o consola y escriba:

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

Pasos siguientes

Tras configurar los servidores adicionales, elimine la copia del archivo de respuesta que utilizó para configurarlos.

Instalar vCloud Director en un miembro adicional de un grupo de servidores

Puede agregar servidores a un grupo de servidores de vCloud Director en cualquier momento. Dado que todos los servidores de un grupo de servidores deben configurarse con los mismos detalles de conexión de base de datos, es necesario utilizar el archivo de respuesta que se creó al configurar el primer miembro del grupo.

Importante No se admiten instalaciones mixtas de vCloud Director en implementaciones de Linux y dispositivos de vCloud Director en un grupo de servidores.

Requisitos previos

- Compruebe que puede acceder al archivo de respuesta que creó cuando configuró el primer miembro del grupo de servidores. Consulte [Configuración de conexiones de red y de base de datos](#).
- Compruebe que montó el almacenamiento de transferencia compartido en el primer miembro del grupo de servidores de vCloud Director en `/opt/vmware/vcloud-director/data/transfer`.

Procedimiento

- 1 Inicie sesión en el servidor de destino como **raíz**.

- 2 Descargue el archivo de instalación en el servidor de destino.

Si ha comprado el software en un medio, copie el archivo de instalación en una ubicación que sea accesible para el servidor de destino.

- 3 Asegúrese de que se pueda ejecutar el archivo de instalación.

El archivo de instalación requiere permiso de ejecución. Para asegurarse de que dispone de dicho permiso, abra una ventana de consola, shell o terminal, y ejecute el siguiente comando Linux, donde *archivo-de-instalación* es el nombre de ruta completo del archivo de instalación de vCloud Director.

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

- 4 Ejecute el archivo de instalación.

Para ejecutar el archivo de instalación, introduzca el nombre de ruta completo; por ejemplo:

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

El archivo incluye un script de instalación y un paquete RPM integrado.

Nota No se puede ejecutar el archivo de instalación desde un directorio cuya ruta de acceso incluya espacios integrados.

Si no instaló la clave pública de VMware en el servidor de destino, el instalador imprime una advertencia con el siguiente formato:

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

El instalador realiza las siguientes acciones.

- a Comprueba que el host cumpla con todos los requisitos.
- b Verifica la firma digital del archivo de instalación.
- c Crea el usuario y el grupo `vcld`.
- d Desempaqueta el paquete RPM de vCloud Director.
- e Instala el software.

Después de completar la instalación, el instalador le indicará que ejecute el script de configuración para configurar las conexiones de red y de base de datos.

- 5 Introduzca **n** y presione Intro para rechazar la ejecución del script de configuración.

Puede ejecutar el script de configuración más adelante si proporciona el archivo de respuesta como entrada.

- 6 Monte el almacenamiento de transferencia compartido en `/opt/vmware/vcloud-director/data/transfer`.

Todos los servidores de vCloud Director del grupo de servidores deben montar este volumen en el mismo punto de montaje.

- 7 Copie el archivo de respuesta en un lugar donde sea accesible para este servidor.

El usuario raíz debe poder leer todos los directorios en el nombre de ruta al archivo de respuesta.

- 8 Ejecute el script de configuración.

- a Proporcione el nombre de ruta del archivo de respuesta para ejecutar el comando `configure`.

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

El script copia el archivo de respuesta en una ubicación que `vcloud.vcloud` pueda leer y ejecuta el script de configuración con el archivo de respuesta como entrada.

- b En los mensajes, proporcione las direcciones IP para el servicio HTTP y el servicio de proxy de la consola.
- c Si el script de configuración no encuentra certificados válidos en el nombre de ruta guardado en el archivo de respuesta, cuando se le solicite, proporcione la ruta de acceso a los certificados y las contraseñas.

El script valida la información, conecta el servidor a la base de datos y ofrece iniciar la celda de vCloud Director.

- 9 (opcional) Introduzca `y` para iniciar el servicio de vCloud Director.

Para iniciar el servicio en otro momento, puede ejecutar el comando `service vmware-vcd start`.

Pasos siguientes

Repita este procedimiento para añadir más servidores a este grupo de servidores.

Después de que los servicios de vCloud Director se encuentren en ejecución en todos los servidores, debe inicializar la base de datos de vCloud Director con una clave de licencia, una cuenta de administrador del sistema y la información relacionada. Puede inicializar la base de datos de una de estas formas:

- Con un explorador web, abra el asistente para la instalación en la dirección URL que se muestra al completarse el script de configuración. Consulte [Configurar vCloud Director](#).
- Utilice la herramienta de administración de celdas con el subcomando `system-setup`. Para obtener información sobre el uso de la herramienta de administración de celdas, consulte *Guía del administrador de vCloud Director*.

Configurar vCloud Director

Después de instalar y configurar todos los servidores en el grupo de servidores de vCloud Director, debe configurar su instalación de vCloud Director. El programa de instalación de vCloud

Director inicializa la base de datos de vCloud Director con una clave de licencia, la cuenta de administrador del sistema y la información relacionada.

Antes de iniciar la consola web de vCloud Director, ejecute el asistente **Instalación de VMware vCloud Director**, que recopila la información que la consola web requiere para iniciarse.

Como alternativa a usar el asistente **Instalación de VMware vCloud Director**, para configurar la instalación de vCloud Director, puede utilizar el subcomando `system-setup` de la herramienta de administración de celdas. Para obtener información sobre esta herramienta, consulte la *Guía del administrador de vCloud Director*.

Requisitos previos

- Compruebe que los servicios de vCloud Director se inician en todos los servidores.
- Obtenga un número de serie de producto de vCloud Director en el Portal de licencias de VMware.

Procedimiento

Procedimiento

- 1 Abra un explorador web y vaya a la dirección URL mostrada en el script de configuración.

Para detectar la dirección URL del asistente **Instalación de VMware vCloud Director**, también puede buscar el nombre de dominio completo asociado a la dirección IP que especificó para el servicio HTTP durante la instalación del primer servidor. Para conectarse con el asistente, vaya a `https://fully-qualified-domain-name`, por ejemplo, `https://mycloud.example.com`.

Nota El inicio del asistente puede tardar unos minutos.

- 2 Revise la página de inicio y haga clic en **Siguiente**.
- 3 Lea y acepte el acuerdo de licencia, y haga clic en **Siguiente**.

Si rechaza el acuerdo de licencia, no puede continuar con la configuración de vCloud Director.

- 4 Introduzca su número de serie de producto de vCloud Director y haga clic en **Siguiente**.
- 5 Introduzca un nombre de usuario, la contraseña y la información de contacto del administrador del sistema de vCloud Director y haga clic en **Siguiente**.

El administrador del sistema de vCloud Director tiene privilegios de superusuario en toda la nube. Este administrador del sistema puede crear cuentas de administrador del sistema adicionales.

- 6 Configure los ajustes del sistema que controlan el modo en que vCloud Director interactúa con vSphere y NSX Manager; a continuación, haga clic en **Siguiente**.
 - a En el cuadro de texto **Nombre del sistema**, introduzca un nombre para la carpeta de vCenter Server que se utilizará en esta instalación de vCloud Director.
 - b En el cuadro de texto **Id. de instalación**, establezca el identificador de esta instalación de vCloud Director para usar al crear direcciones MAC para NIC virtuales.

Si tiene pensado crear redes extendidas en las instalaciones de vCloud Director en implementaciones multisitio, considere la posibilidad de definir un identificador de instalación único para cada instalación de vCloud Director.
- 7 En la página Listo para iniciar sesión, revise la configuración y haga clic en **Finalizar**.

Resultados

Cuando finalice el proceso de configuración, el sistema lo redirigirá a la página de inicio de sesión de la consola web de vCloud Director.

Pasos siguientes

Inicie sesión en la consola web de vCloud Director con el nombre de usuario del administrador del sistema y la contraseña, y comience a aprovisionar su nube. Para obtener información sobre cómo agregar recursos a vCloud Director, consulte la *Guía del administrador de vCloud Director*.

Implementar el dispositivo de vCloud Director

6

Puede crear un grupo de servidores de vCloud Director mediante la implementación de una o varias instancias del dispositivo de vCloud Director. Implemente el dispositivo de vCloud Director mediante vSphere Client (HTML5), vSphere Web Client (Flex) o VMware OVF Tool.

Importante No se admiten instalaciones mixtas de vCloud Director en implementaciones de Linux y dispositivos de vCloud Director en un grupo de servidores.

El dispositivo de vCloud Director es una máquina virtual preconfigurada optimizada para ejecutar los servicios de vCloud Director.

El dispositivo se distribuye con un nombre con el formato VMware vCloud Director-*v.v.v.v-nnnnnn*_OVF10.ova, donde *v.v.v.v* representa la versión de producto y *nnnnnn*, el número de compilación. Por ejemplo: VMware vCloud Director-9.7.0.0-9229800_OVA10.ova.

El paquete del dispositivo de vCloud Director contiene el siguiente software:

- Sistema operativo VMware Photon™
- El grupo de servicios de vCloud Director
- PostgreSQL 10

Los tamaños del dispositivo de vCloud Director principal-pequeño y en espera-pequeño son adecuados para los sistemas de laboratorio o de pruebas. Los tamaños principal-grande y en espera-grande cumplen los requisitos mínimos de tamaño para los sistemas de producción. En función de la carga de trabajo, es posible que tenga que agregar más recursos.

Importante No se admite la instalación de ningún componente de terceros en el dispositivo de vCloud Director. Puede instalar solo componentes de VMware compatibles según las [Matrices de interoperabilidad de productos de VMware](#). Por ejemplo, puede instalar una versión compatible de un VMware vRealize® Operations Manager™ o un agente de supervisión de VMware vRealize® Log Insight™.

Configuración de base de datos del dispositivo

A partir de la versión 9.7, el dispositivo de vCloud Director incluye una base de datos de PostgreSQL integrada con una función de alta disponibilidad (high availability, HA). Para crear una implementación de dispositivo con un clúster de HA de base de datos, debe implementar una instancia del dispositivo de vCloud Director como celda principal y dos instancias como celdas en espera. Puede implementar instancias adicionales del dispositivo de vCloud Director en el grupo de servidores como celdas de aplicación de vCD, las cuales solo ejecutan el grupo de servicios de vCloud Director sin la base de datos integrada. Las celdas de aplicación de vCD se conectan con la base de datos en la celda principal. Consulte [Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos](#).

Para las conexiones de base de datos, incluida la replicación, el dispositivo de vCloud Director utiliza TLS de forma predeterminada, en lugar de la opción SSL (la cual está obsoleta). Esta función está activa inmediatamente después de la implementación, mediante un certificado de PostgreSQL autofirmado. Para utilizar un certificado firmado de una entidad de certificación (Certificate Authority, CA), consulte [Reemplazar un certificado autofirmado de interfaz de usuario de administración de dispositivos de vCloud Director y de una instancia integrada de PostgreSQL](#).

Nota El dispositivo de vCloud Director no admite bases de datos externas.

Configuración de red del dispositivo

A partir de la versión 9.7, el dispositivo de vCloud Director se implementa con dos redes, eth0 y eth1, para que sea posible aislar el tráfico HTTP del tráfico de base de datos. Los diferentes servicios escuchan en una o las dos interfaces de red correspondientes.

Servicio	Puerto en eth0	Puerto en eth1
SSH	22	22
HTTP	80	N/A
HTTPS	443	N/A
PostgreSQL	N/A	5432
Interfaz de usuario de administración	5480	5480
Proxy de consola	8443	N/A
JMX	8998, 8999	N/A
JMS/ActiveMQ	61616	N/A

El dispositivo de vCloud Director admite que el usuario personalice las reglas de firewall mediante iptables. Para agregar reglas de iptables personalizadas, puede agregar sus propios datos de configuración al final del archivo /etc/systemd/scripts/iptables.

Este capítulo incluye los siguientes temas:

- [Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos](#)

- [Requisitos previos para implementar el dispositivo de vCloud Director](#)
- [Implementar el dispositivo de vCloud Director mediante vSphere Web Client o vSphere Client](#)
- [Implementar el dispositivo de vCloud Director mediante VMware OVF Tool](#)

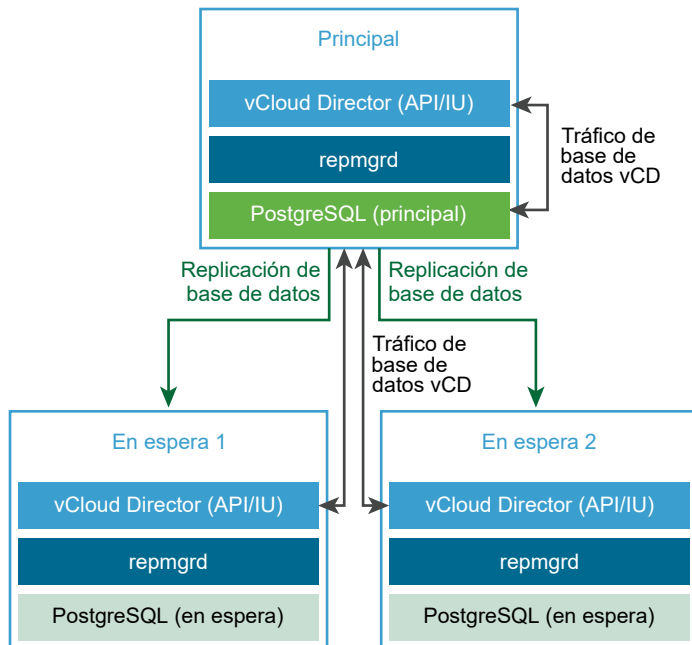
Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos

El dispositivo de vCloud Director incluye una base de datos de PostgreSQL integrada. La base de datos de PostgreSQL integrada incluye el conjunto de herramientas de Replication Manager (repmgr), que proporciona una función de alta disponibilidad (High Availability, HA) a un clúster de servidores de PostgreSQL. Es posible crear una implementación de dispositivo con un clúster de HA de base de datos que proporcione capacidades de conmutación por error a la base de datos de vCloud Director.

Se puede implementar el dispositivo de vCloud Director como celda principal, celda en espera o celda de aplicación de vCD. Consulte [Implementar el dispositivo de vCloud Director mediante vSphere Web Client o vSphere Client](#), [Implementar el dispositivo de vCloud Director mediante VMware OVF Tool](#) o [Implementar el dispositivo de vCloud Director con certificados comodín firmados para las comunicaciones de proxy de consola y HTTPS](#).

Para configurar HA para la base de datos de vCloud Director, al crear el grupo de servidores, puede implementar una instancia principal y dos instancias en espera del dispositivo de vCloud Director para configurar un clúster de HA de base de datos.

Figura 6-1. Un clúster de HA de base de datos en dispositivo de vCloud Director



Crear una implementación de dispositivo de vCloud Director con HA de base de datos

Para crear un grupo de servidores de vCloud Director con una configuración de HA de base de datos, siga este flujo de trabajo:

- 1 Implemente el dispositivo de vCloud Director como celda principal.

La celda principal es el primer miembro del grupo de servidores de vCloud Director. La base de datos integrada se configura como la base de datos de vCloud Director. El nombre de la base de datos es `vcld` y el usuario de la base de datos es `vcld`.

- 2 Compruebe que la celda principal esté lista y en ejecución.

- a Para comprobar el estado del servicio de vCloud Director, inicie sesión con las credenciales de **administrador del sistema** en la consola web de vCloud Director en `https://primary_eth0_ip_address/cloud`.
- b Para comprobar el estado de la base de datos PostgreSQL, inicie sesión como **usuario raíz** en la interfaz de usuario de administración de dispositivos en `https://primary_eth1_ip_address:5480`.

El nodo principal debe estar en estado de ejecución.

- 3 Implemente dos instancias del dispositivo de vCloud Director como celdas en espera.

Las bases de datos integradas se configuran en modo de replicación con la base de datos principal.

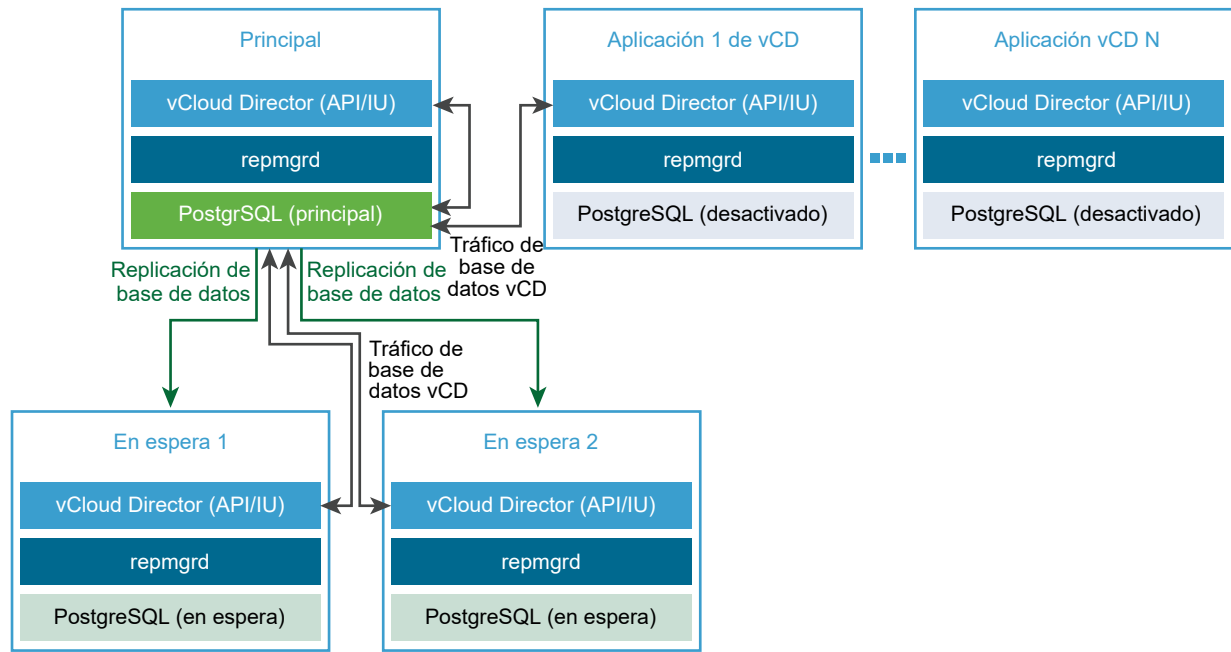
Nota Después de la implementación inicial del dispositivo en espera, Replication Manager comienza a sincronizar su base de datos con la base de datos del dispositivo principal. Durante este período, la base de datos de vCloud Director y, por tanto, la interfaz de usuario de vCloud Director no están disponibles.

- 4 Compruebe que todas las celdas del clúster de HA estén en ejecución.

Consulte [Ver el estado de las celdas en un clúster de alta disponibilidad de la base de datos](#).

- 5 (Opcional) Implemente una o varias instancias del dispositivo de vCloud Director como celdas de aplicación de vCD.

Las bases de datos integradas no se utilizan. La celda de aplicación de vCD se conecta a la base de datos principal.



Crear una implementación de dispositivo de vCloud Director sin HA de base de datos

Para crear un servidor de vCloud Director sin una configuración de HA de base de datos, siga este flujo de trabajo:

- 1 Implemente el dispositivo de vCloud Director como celda principal.

La celda principal es el primer miembro del grupo de servidores de vCloud Director. La base de datos integrada se configura como la base de datos de vCloud Director. El nombre de la base de datos es `vc1oud` y el usuario de la base de datos es `vc1oud`.

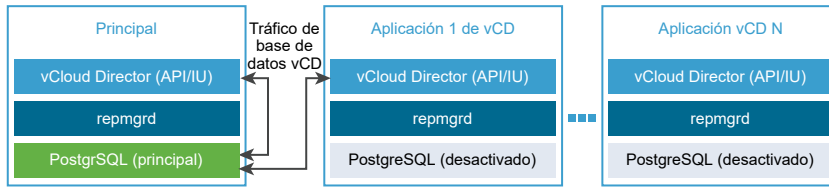
- 2 Compruebe que la celda principal esté lista y en ejecución.

- a Para comprobar el estado del servicio de vCloud Director, inicie sesión con las credenciales de **administrador del sistema** en la consola web de vCloud Director en `https://primary_eth0_ip_address/cloud`.
- b Para comprobar el estado de la base de datos PostgreSQL, inicie sesión como **usuario raíz** en la interfaz de usuario de administración de dispositivos en `https://primary_eth1_ip_address:5480`.

El nodo principal debe estar en estado de ejecución.

- 3 (Opcional) Implemente una o varias instancias del dispositivo de vCloud Director como celdas de aplicación de vCD.

La base de datos integrada no se utiliza. La celda de aplicación de vCD se conecta a la base de datos principal.



Requisitos previos para implementar el dispositivo de vCloud Director

Para garantizar la correcta implementación del dispositivo de vCloud Director, debe realizar algunas tareas y comprobaciones previas obligatorias antes de iniciar la implementación.

- Compruebe que tiene acceso al archivo .ova de vCloud Director.
- Antes de implementar el dispositivo principal, prepare un almacenamiento de servicio de transferencia compartido de NFS. Consulte [Preparar el almacenamiento del servidor de transferencia](#).

Nota El almacenamiento de servicio de transferencia compartido no debe contener ningún archivo `responses.properties` o directorio `appliance-nodes`.

- [Instalar y configurar un agente AMQP de RabbitMQ.](#)

Métodos de implementación del dispositivo de vCloud Director

- [Implementar el dispositivo de vCloud Director mediante vSphere Web Client o vSphere Client](#)
- [Implementar el dispositivo de vCloud Director mediante VMware OVF Tool](#)
- [Implementar el dispositivo de vCloud Director con certificados comodín firmados para las comunicaciones de proxy de consola y HTTPS](#)

Implementar el dispositivo de vCloud Director mediante vSphere Web Client o vSphere Client

Es posible implementar el dispositivo vCloud Director como una plantilla de OVF mediante vSphere Web Client (Flex) o vSphere Client (HTML5).

Es necesario implementar el primer miembro de un grupo de servidores de vCloud Director como celda principal. Es posible implementar un miembro subsiguiente de un grupo de servidores de vCloud Director como celda en espera o de aplicación de vCD. Consulte [Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos](#).

Importante No se admiten instalaciones mixtas de vCloud Director en implementaciones de Linux y dispositivos de vCloud Director en un grupo de servidores.

Para obtener información sobre la implementación de plantillas de OVF en vSphere, consulte *Administrar máquinas virtuales de vSphere*.

Como alternativa, puede implementar el dispositivo mediante VMware OVF Tool. Consulte [Implementar el dispositivo de vCloud Director mediante VMware OVF Tool](#).

Nota No se admite la implementación de un dispositivo de vCloud Director en vCloud Director.

Requisitos previos

Consulte [Requisitos previos para implementar el dispositivo de vCloud Director](#).

Procedimiento

1 Iniciar la implementación del dispositivo de vCloud Director

Para iniciar la implementación del dispositivo, abra el asistente de implementación en vSphere Web Client (Flex) o vSphere Client (HTML5).

2 Personalizar el dispositivo de vCloud Director y finalizar la implementación

Para configurar los detalles de vCloud Director, debe personalizar la plantilla de dispositivo.

Pasos siguientes

- Configure la dirección de proxy de la consola pública, ya que el dispositivo de vCloud Director utiliza su NIC eth0 con el puerto personalizado 8443 para el servicio de proxy de la consola. Consulte [Personalizar endpoints públicos](#).
- Para agregar miembros al grupo de servidores de vCloud Director, repita el procedimiento.
- Para introducir la clave de licencia, inicie sesión en la consola web de vCloud Director.
- Para reemplazar el certificado autofirmado que se crea durante el primer arranque del dispositivo, puede [Crear un almacén de claves de certificados SSL firmados por una entidad de certificación para vCloud Director en Linux](#).

Iniciar la implementación del dispositivo de vCloud Director

Para iniciar la implementación del dispositivo, abra el asistente de implementación en vSphere Web Client (Flex) o vSphere Client (HTML5).

Procedimiento

- 1 En vSphere Web Client o vSphere Client, haga clic con el botón derecho en cualquier objeto de inventario y haga clic en **Implementar plantilla de OVF**.
- 2 Introduzca la ruta de acceso al archivo .ova de vCloud Director y haga clic en **Siguiente**.
- 3 Introduzca un nombre para la máquina virtual, examine el repositorio de vCenter Server para seleccionar el centro de datos o la carpeta donde desea implementar el dispositivo y haga clic en **Siguiente**.
- 4 Seleccione el host ESXi o el clúster donde desea implementar el dispositivo y haga clic en **Siguiente**.

- 5 Revise los detalles de la plantilla y haga clic en **Siguiente**.
- 6 Lea y acepte los contratos de licencia, y haga clic en **Siguiente**.
- 7 Seleccione el tipo y el tamaño de implementación, y haga clic en **Siguiente**.

Los tamaños del dispositivo de vCloud Director principal-pequeño y en espera-pequeño son adecuados para los sistemas de laboratorio o de pruebas. Los tamaños principal-grande y en espera-grande cumplen los requisitos mínimos de tamaño para los sistemas de producción. En función de la carga de trabajo, es posible que tenga que agregar más recursos.

Opción	Descripción
Principal-pequeña	<p>Implementa el dispositivo con 12 GB de RAM y 2 vCPU como el primer miembro en un grupo de servidores de vCloud Director.</p> <p>La base de datos integrada en la celda principal se configura como la base de datos de vCloud Director. El nombre de la base de datos es vcloud y el usuario de la base de datos es vcloud.</p>
Principal-grande	<p>Implementa el dispositivo con 24 GB de RAM y 4 vCPU como el primer miembro en un grupo de servidores de vCloud Director.</p> <p>La base de datos integrada en la celda principal se configura como la base de datos de vCloud Director. El nombre de la base de datos es vcloud y el usuario de la base de datos es vcloud.</p>
En espera-pequeña	<p>Se usa para unir una celda principal-pequeña en un clúster de HA de base de datos.</p> <p>Implementa el dispositivo con 12 GB de RAM y 2 vCPU como segundo o tercer miembro en un grupo de servidores de vCloud Director con una configuración de alta disponibilidad de base de datos.</p> <p>La base de datos integrada en una celda en espera se configura en modo de replicación con la base de datos principal.</p>
En espera-grande	<p>Se usa para unir una celda principal-grande en un clúster de HA de base de datos.</p> <p>Implementa el dispositivo con 24 GB de RAM y 4 vCPU como segundo o tercer miembro en un grupo de servidores de vCloud Director con una configuración de alta disponibilidad de base de datos.</p> <p>La base de datos integrada en un dispositivo en espera se configura en modo de replicación con la base de datos principal.</p>
Celda de aplicación de vCD	<p>Implementa el dispositivo con 8 GB de RAM y 2 vCPU como miembro subsiguiente en un grupo de servidores de vCloud Director.</p> <p>La base de datos integrada en una celda de aplicación de vCD no se utiliza. La celda de aplicación de vCD se conecta a la base de datos principal.</p>

Importante Las celdas principal y en espera de un grupo de servidores de vCloud Director deben tener el mismo tamaño. Un clúster de HA de base de datos puede incluir una celda principal-pequeña y dos celdas en espera-pequeñas, o bien una celda principal-grande y dos celdas en espera-grandes.

Después de la implementación, puede volver a configurar el tamaño del dispositivo.

- 8 Seleccione el formato de disco y el almacén de datos para los archivos de configuración de las máquinas virtuales y los discos virtuales, y haga clic en **Siguiente**.

Los formatos gruesos mejoran el rendimiento y los formatos finos permiten ahorrar espacio de almacenamiento.

- 9 En los menús desplegables de las celdas **Red de destino**, seleccione las redes de destino para las NIC eth1 y eth0 del dispositivo.

La lista de red de origen puede estar en orden inverso. Asegúrese de seleccionar la red de destino correcta para cada red de origen.

Importante Las dos redes de destino deben ser diferentes.

- 10 En los menús desplegables de **Configuración de asignación**, seleccione la asignación de IP **Estática-manual** y el protocolo **IPv4**.

- 11 Haga clic en **Siguiente**.

Será redirigido a la página **Personalizar plantilla** para configurar los detalles de vCloud Director.

Personalizar el dispositivo de vCloud Director y finalizar la implementación

Para configurar los detalles de vCloud Director, debe personalizar la plantilla de dispositivo.

Cuando se personaliza el dispositivo de vCloud Director, se configuran las opciones, la base de datos y las propiedades de red del dispositivo. La configuración inicial del sistema solo se realiza cuando se implementa un dispositivo principal, que es el primer miembro de un grupo de servidores.

Nota Solo es opcional el [Paso 3](#) de este procedimiento. Debe completar todos los pasos restantes para personalizar el dispositivo de vCloud Director.

Procedimiento

- 1 En la sección **Configuración del dispositivo de VCD**, configure los detalles del dispositivo.

Configuración	Descripción
Servidor NTP	El nombre de host o la dirección IP del servidor NTP que se usará.
Contraseña raíz inicial	<p>La contraseña raíz inicial para el dispositivo. Debe contener al menos ocho caracteres, un carácter en mayúscula, un carácter en minúscula, un dígito numérico y un carácter especial.</p> <p>Importante La contraseña raíz inicial se convierte en la contraseña del almacén de claves. La implementación del clúster requiere que todas las celdas tengan la misma contraseña raíz durante la implementación inicial. Una vez que finalice el proceso de arranque, puede cambiar la contraseña raíz en cualquier celda que desee.</p> <p>Nota El asistente de implementación de OVF no valida la contraseña raíz inicial con los criterios de contraseña.</p>
Caducar contraseña raíz después de primer inicio de sesión	Si desea continuar usando la contraseña inicial después del primer inicio de sesión, debe comprobar que la contraseña inicial cumpla con los criterios de contraseña raíz. Para continuar usando la contraseña raíz inicial después del primer inicio de sesión, anule la selección de esta opción.
Habilitar SSH	Opción deshabilitada de forma predeterminada.
Montaje de NFS para la ubicación del archivo de transferencia	Consulte Preparar el almacenamiento del servidor de transferencia .

Nota Para obtener información sobre cómo cambiar la fecha, la hora o la zona horaria del dispositivo, consulte <https://kb.vmware.com/kb/59674>.

- 2 Si desea implementar el primer miembro de un grupo de servidores, en la sección **Configurar VCD - Solo se requiere para dispositivos "principales"**, introduzca los detalles de la base de datos, cree la cuenta de **administrador del sistema** y configure las opciones del sistema.

El nombre de la base de datos es vcloud y el usuario de la base de datos es vcloud.

Configuración	Descripción
Contraseña de la base de datos "vCloud" para el usuario "vCloud"	La contraseña para el usuario de la base de datos vcloud.
Nombre del usuario administrador	El nombre de usuario para la cuenta de administrador del sistema . De forma predeterminada, es administrator.
Nombre completo del administrador	El nombre completo del administrador del sistema . De forma predeterminada, es vCD Admin.
Contraseña del usuario administrador	La contraseña para la cuenta de administrador del sistema .
Correo electrónico del administrador	La dirección de correo electrónico del administrador del sistema .

Configuración	Descripción
Nombre del sistema	El nombre de la carpeta de vCenter Server que se creará para esta instalación de vCloud Director. De forma predeterminada, es vcd1.
Id. de instalación	El identificador de esta instalación de vCloud Director que se utilizará al crear direcciones MAC para NIC virtuales. De forma predeterminada, es 1. Si tiene pensado crear redes extendidas en las instalaciones de vCloud Director en implementaciones multisitio, considere la posibilidad de definir un identificador de instalación único para cada instalación de vCloud Director.

- 3 (opcional) En la sección **Propiedades de redes adicionales**, si la topología de la red lo requiere, introduzca las rutas estáticas para las interfaces de redes eth0 y eth1, y haga clic en **Siguiente**.

Es posible que deba proporcionar rutas estáticas si desea acceder a los hosts a través de una ruta de puerta de enlace no predeterminada. Por ejemplo, solo se puede acceder a la infraestructura de administración a través de la interfaz de eth1, mientras que la puerta de enlace predeterminada está en eth0. En la mayoría de los casos, esta opción puede permanecer vacía.

Las rutas estáticas deben estar en una lista de especificaciones de rutas separadas por comas. Una especificación de ruta debe incluir la dirección IP de la puerta de enlace de destino y, de forma opcional, una especificación de red de enrutamiento de interdominios sin clases (Classless Inter-Domain Routing, CIDR). Por ejemplo,
172.16.100.253 172.16.100.0/19, 172.16.100.253 192.168.100.0/24.

- 4 En la sección **Propiedades de redes**, introduzca los detalles de red para las NIC eth0 y eth1, y haga clic en **Siguiente**.

Nota Todos los ajustes son obligatorios.

Configuración	Descripción
Puerta de enlace predeterminada	La dirección IP de la puerta de enlace predeterminada para el dispositivo.
Nombre de dominio	El nombre de dominio (por ejemplo, <i>midominio.com</i>).
Ruta de búsqueda de dominios	Una lista separada por comas o por espacios de los nombres de dominio para la ruta de búsqueda de dominios del dispositivo.
Servidores de nombres de dominio	La dirección IP del servidor de nombres de dominio para el dispositivo.
Dirección IP de red de eth0	La dirección IP de la interfaz eth0.
Máscara de red de eth0	El prefijo o la máscara de la interfaz eth0.
Dirección IP de red de eth1	La dirección IP de la interfaz eth1.
Máscara de red de eth1	El prefijo o la máscara de la interfaz eth1.

- 5 En la página **Listo para completar**, revise los ajustes de configuración del dispositivo de vCloud Director y haga clic en **Finalizar** para iniciar la implementación.

Pasos siguientes

Encienda la máquina virtual recién creada.

Implementar el dispositivo de vCloud Director mediante VMware OVF Tool

Es posible implementar el dispositivo de vCloud Director como una plantilla de OVF mediante VMware OVF Tool.

Es necesario implementar el primer miembro de un grupo de servidores de vCloud Director como celda principal. Es posible implementar un miembro subsiguiente de un grupo de servidores de vCloud Director como celda en espera o de aplicación de vCD. Consulte [Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos](#).

Para obtener información sobre la instalación de OVF Tool, consulte el documento *Notas de la versión de VMware OVF Tool*.

Para obtener información sobre cómo usar OVF Tool, consulte *Guía del usuario de OVF Tool*.

Antes de ejecutar el comando de implementación, consulte [Requisitos previos para implementar el dispositivo de vCloud Director](#).

Después de implementar el dispositivo, consulte el archivo de log de primer arranque para ver los mensajes de error de advertencia. Consulte [Examinar los archivos de log en el dispositivo de vCloud Director](#).

Propiedades y opciones de comandos de ovftool para implementar el dispositivo de vCloud Director

Opción	Valor	Descripción
--noSSLVerify	N/A	Omite la verificación de SSL para las conexiones de vSphere.
--acceptAllEulas	N/A	Acepta todos los contratos de licencia para el usuario final (CLUF).
--datastore	<i>target_vc_datastore</i>	El nombre del almacén de datos de destino en el que se almacenarán los archivos de configuración de las máquinas virtuales y los discos virtuales.
--allowAllExtraConfig	N/A	Convierte todas las opciones de configuración adicionales al formato VMX.
--net:"eth0 Network"	<i>portgroup_on_vc_for_eth0</i>	La red de destino para la red eth0 del dispositivo. Importante Debe ser diferente de la red de destino eth1.

Opción	Valor	Descripción
<code>--net:"eth1 Network"</code>	<code>portgroup_on_vc_for_eth1</code>	La red de destino para la red eth1 del dispositivo. Importante Debe ser diferente de la red de destino eth0.
<code>--name</code>	<code>vm_name_on_vc</code>	El nombre de la máquina virtual para el dispositivo.
<code>--diskMode</code>	<code>thin</code> o <code>thick</code>	El formato de disco para los archivos de configuración de las máquinas virtuales y los discos virtuales.
<code>--prop:"vami.ip0.VMware_vCloud_Director"</code>	<code>eth0_ip_address</code>	La dirección IP de eth0. Se utiliza para el acceso a la interfaz de usuario y a la API. En esta dirección, la búsqueda inversa de DNS determina y establece el nombre de host del dispositivo.
<code>--prop:"vami.ip1.VMware_vCloud_Director"</code>	<code>eth1_ip_address</code>	La dirección IP de eth1. Se utiliza para acceder a los servicios internos, incluido el servicio de base de datos de PostgreSQL integrada.
<code>--prop:"vami.DNS.VMware_vCloud_Director"</code>	<code>dns_ip_address</code>	La dirección IP del servidor de nombres de dominio para el dispositivo.
<code>--prop:"vami.domain.VMware_vCloud_Director"</code>	<code>domain_name</code>	El dominio de búsqueda de DNS. Aparece como el primer elemento en la ruta de búsqueda.
<code>--prop:"vami.gateway.VMware_vCloud_Director"</code>	<code>gateway_ip_address</code>	La dirección IP de la puerta de enlace predeterminada para el dispositivo.
<code>--prop:"vami.netmask0.VMware_vCloud_Director"</code>	<code>netmask</code>	El prefijo o la máscara de la interfaz eth0.
<code>--prop:"vami.netmask1.VMware_vCloud_Director"</code>	<code>netmask</code>	El prefijo o la máscara de la interfaz eth1.
<code>--prop:"vami.searchpath.VMware_vCloud_Director"</code>	<code>list_of_domain_names</code>	La ruta de búsqueda de dominios del dispositivo. Una lista de nombres de dominio separados por espacios o por comas.
<code>--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"</code>	<code>true</code> o <code>false</code>	Habilita o deshabilita el acceso SSH root al dispositivo.
<code>--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"</code>	<code>minutes</code>	Determina si se debe continuar usando o no la contraseña inicial después del primer inicio de sesión.
<code>--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"</code>	<code>ip_address:nfs_mount_path</code>	La dirección IP y la ruta de exportación del servidor NFS externo. Solo se usa para una celda principal.
<code>--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"</code>	<code>ntp_server_ip_address</code>	La dirección IP del servidor de tiempo.

Opción	Valor	Descripción
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"	vcloudapp.varoot-password	La contraseña raíz inicial para el dispositivo. Debe contener al menos ocho caracteres, un carácter en mayúscula, un carácter en minúscula, un dígito numérico y un carácter especial. Importante La contraseña raíz inicial se convierte en la contraseña del almacén de claves. La implementación del clúster requiere que todas las celdas tengan la misma contraseña raíz durante la implementación inicial. Una vez que finalice el proceso de arranque, puede cambiar la contraseña raíz en cualquier celda que desee.
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"	vcloudconf.db_pwd	La contraseña de la base de datos del usuario vcloud . Solo se usa para una celda principal.
--prop:"vcloudwiz.admin_email.VMware_vCloud_Director"	vcloudwiz.admin_email	La dirección de correo electrónico de la cuenta de administrador del sistema . Solo se usa para una celda principal.
--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director"	vcloudwiz.admin_fname	El nombre para la cuenta de administrador del sistema . Solo se usa para una celda principal.
--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director"	vcloudwiz.admin_pwd	La contraseña para la cuenta de administrador del sistema . Solo se usa para una celda principal.
--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director"	vcloudwiz.admin_uname	El nombre de usuario para la cuenta de administrador del sistema . Solo se usa para una celda principal.
--prop:"vcloudwiz.inst_id.VMware_vCloud_Director"	vcloudwiz.inst_id	El identificador de instalación de vCloud Director. Solo se usa para una celda principal.
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"	vcloudconf.sys_name	El nombre de la carpeta de vCenter Server que se creará para esta instalación de vCloud Director.

Opción	Valor	Descripción
<code>--prop:"vcloudnet.routes0.VMware_vCloud_Director_directness1 cidr, ip_address2, ...</code>	<code>directness1 cidr, ip_address2, ...</code>	Opcional. Las rutas estáticas para la interfaz eth0. Debe ser una lista de especificaciones de ruta separadas por comas. Una especificación de ruta debe constar de una dirección IP de puerta de enlace y, de forma opcional, una especificación de red de enrutamiento de interdominios sin clases (Classless Inter-Domain Routing, CIDR) (prefijo/bits). Por ejemplo, 172.16.100.253 172.16.100/19, 172.16.200.253.
<code>--prop:"vcloudnet.routes1.VMware_vCloud_Director_directness1 cidr, ip_address2, ...</code>	<code>directness1 cidr, ip_address2, ...</code>	Opcional. Las rutas estáticas para la interfaz eth1. Debe ser una lista de especificaciones de ruta separadas por comas. Una especificación de ruta debe constar de una dirección IP de puerta de enlace y, de forma opcional, una especificación de red de enrutamiento de interdominios sin clases (Classless Inter-Domain Routing, CIDR) (prefijo/bits). Por ejemplo, 172.16.100.253 172.16.100/19, 172.16.200.253.

Opción	Valor	Descripción
--deploymentOption	primary-small,primary-large, standby-small, standby-large o cell	<p>El tipo y el tamaño de dispositivo que desea implementar.</p> <p>Los tamaños del dispositivo principal-pequeño y en espera-pequeño son adecuados para los sistemas de laboratorio o de pruebas. Los tamaños principal-grande y en espera-grande cumplen los requisitos mínimos de tamaño para los sistemas de producción. En función de la carga de trabajo, es posible que tenga que agregar más recursos.</p> <ul style="list-style-type: none"> ■ primary-small implementa el dispositivo con 12 GB de RAM y 2 vCPU como el primer miembro en un grupo de servidores de vCloud Director. La base de datos integrada en la celda principal se configura como la base de datos de vCloud Director. El nombre de la base de datos es vcloud y el usuario de la base de datos es vcloud. ■ primary-large implementa el dispositivo con 24 GB de RAM y 4 vCPU como el primer miembro en un grupo de servidores de vCloud Director. La base de datos integrada en la celda principal se configura como la base de datos de vCloud Director. El nombre de la base de datos es vcloud y el usuario de la base de datos es vcloud. ■ standby-small implementa el dispositivo con 12 GB de RAM y 2 vCPU como segundo o tercer miembro en un grupo de servidores de vCloud Director con una configuración de alta disponibilidad de base de datos. La base de datos integrada en una celda en espera se configura en modo de replicación con la base de datos principal. ■ standby-large implementa el dispositivo con 24 GB de RAM y 4 vCPU como segundo o tercer miembro en un grupo de servidores de vCloud Director con una configuración de alta disponibilidad de base de datos. La

Opción	Valor	Descripción
		<p>base de datos integrada en una celda en espera se configura en modo de replicación con la base de datos principal.</p> <ul style="list-style-type: none"> ■ cell implementa el dispositivo con 8 GB de RAM y 2 vCPU como miembro subsiguiente en un grupo de servidores de vCloud Director. La base de datos integrada en una celda de aplicación de vCD no se utiliza. La celda de aplicación de vCD se conecta a la base de datos principal. <p>Importante Las celdas principal y en espera de un grupo de servidores de vCloud Director deben tener el mismo tamaño. Un clúster de HA de base de datos puede incluir una celda principal-pequeña y dos celdas en espera-pequeñas, o bien una celda principal-grande y dos celdas en espera-grandes.</p> <p>Después de la implementación, puede volver a configurar el tamaño del dispositivo.</p>
--powerOn	<i>path_to_ova</i>	Enciende la máquina virtual después de completarse la implementación.

Un comando de ejemplo para implementar el dispositivo principal de vCloud Director

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
```

```
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="Xj052mXAP7n#" \
--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"="o@e@vJW26Pnb" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

Un comando de ejemplo para implementar un dispositivo en espera de vCloud Director

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="44z1Bd1HwIt#" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \
--deploymentOption="standby-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

Creación y administración de certificados SSL del dispositivo vCloud Director

7

El dispositivo de vCloud Director usa SSL para proteger la comunicación entre clientes y servidores. Cada dispositivo de vCloud Director debe admitir dos endpoints de SSL diferentes: uno para HTTPS y otro para comunicaciones de proxy de consola.

Estos endpoints pueden ser direcciones IP separadas o una única dirección IP con dos puertos diferentes. Cada extremo requiere su propio certificado SSL. Puede utilizar el mismo certificado (por ejemplo, un certificado comodín) para ambos endpoints.

Este capítulo incluye los siguientes temas:

- Implementar el dispositivo de vCloud Director con certificados comodín firmados para las comunicaciones de proxy de consola y HTTPS
- Crear e importar certificados SSL firmados por una entidad de certificación para el dispositivo de vCloud Director
- Importar claves privadas y certificados SSL firmados por una entidad de certificación en el dispositivo de vCloud Director
- Reemplazar un certificado autofirmado de interfaz de usuario de administración de dispositivos de vCloud Director y de una instancia integrada de PostgreSQL
- Renovar los certificados del dispositivo de vCloud Director

Implementar el dispositivo de vCloud Director con certificados comodín firmados para las comunicaciones de proxy de consola y HTTPS

Puede implementar el dispositivo de vCloud Director con certificados comodín firmados. Puede utilizar estos certificados para proteger una cantidad ilimitada de servidores que son subdominios del nombre de dominio que aparece en el certificado.

De forma predeterminada, cuando se implementan dispositivos de vCloud Director, vCloud Director genera certificados autofirmados y configura con ellos la celda de vCloud Director para las comunicaciones de proxy de consola y HTTPS.

Cuando se implementa correctamente un dispositivo principal, la lógica de configuración del dispositivo copia el archivo `responses.properties` del dispositivo principal en el almacenamiento común del servicio de transferencia compartido de NFS en `/opt/vmware/vcloud-director/data/transfer`. Con este archivo, otros dispositivos implementados para este grupo de vCloud Director Servers se autoconfiguran automáticamente. El archivo `responses.properties` incluye una ruta de acceso al almacén de claves de certificados SSL, que incluye los certificados autofirmados y generados automáticamente `user.keystore.path`. De forma predeterminada, esta ruta de acceso lleva a un archivo de almacén de claves que es local para cada dispositivo.

Después de implementar el dispositivo principal, puede volver a configurarlo para utilizar certificados firmados. Para obtener más información sobre cómo crear el almacén de claves con certificados firmados, consulte [Crear e importar certificados SSL firmados por una entidad de certificación para el dispositivo de vCloud Director](#).

Si los certificados firmados que utiliza en el dispositivo principal de vCloud Director son certificados comodín firmados, estos certificados pueden aplicarse a todos los demás dispositivos del grupo de servidores de vCloud Director (es decir, celdas en espera y celdas de aplicación de vCloud Director). Puede utilizar la implementación del dispositivo con certificados comodín firmados para comunicaciones de proxy de consola y HTTPS con el fin de configurar las celdas adicionales con los certificados comodín SSL firmados.

Requisitos previos

- Compruebe que el almacén de claves que contiene los certificados comodín SSL firmados para los alias de proxy de consola y HTTPS esté disponible en el dispositivo principal (es decir, `/opt/vmware/vcloud-director/certificates.ks`).
 - Si necesita crear pares de claves e importar archivos de certificados firmados por una entidad de certificación, consulte [Crear e importar certificados SSL firmados por una entidad de certificación para el dispositivo de vCloud Director](#).
 - Si ya dispone de una clave privada y de archivos de certificados firmados por una entidad de certificación propios, consulte [Importar claves privadas y certificados SSL firmados por una entidad de certificación en el dispositivo de vCloud Director](#).
- Compruebe que la contraseña privada de las claves en el almacén de claves coincida con la contraseña del almacén de claves. La contraseña del almacén de claves debe coincidir con la contraseña raíz inicial que se utiliza al implementar todos los dispositivos, por ejemplo:

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

Procedimiento

- 1 Copie el nuevo archivo `certificates.ks` que contiene los certificados firmados correctamente del dispositivo principal al recurso compartido de transferencia en `/opt/vmware/vcloud-director/data/transfer/`.

- 2 Cambie los permisos de propietario y de grupo en el archivo de almacén de claves a **vcloud**.

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

- 3 Compruebe que el propietario del archivo de almacén de claves tiene permisos de lectura y escritura.

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

- 4 En el dispositivo principal, ejecute el comando para importar los nuevos certificados firmados en la instancia de vCloud Director.

Este comando también actualiza el archivo `responses.properties` en el recurso compartido de transferencia, lo que modifica la variable `user.keystore.path` para que apunte al archivo de almacén de claves en el recurso compartido de transferencia.

```
/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 Para que se apliquen los nuevos certificados firmados, reinicie el servicio `vmware-vcd` en el dispositivo principal.

```
service vmware-vcd restart
```

- 6 Implemente los dispositivos de celda de aplicación y celda en espera mediante la contraseña raíz inicial que coincide con la contraseña del almacén de claves.

Resultados

Todos los dispositivos recién implementados que utilizan el mismo almacenamiento de servicio de transferencia compartido de NFS se configuran con los mismos certificados comodín SSL firmados que el dispositivo principal utiliza.

Crear e importar certificados SSL firmados por una entidad de certificación para el dispositivo de vCloud Director

La creación y la importación de certificados firmados por una entidad de certificación proporcionan el nivel más alto de confianza para las comunicaciones de SSL y ayudan a proteger las conexiones dentro de la nube.

Cada servidor de vCloud Director requiere dos certificados SSL para proteger las comunicaciones entre los clientes y los servidores. Cada servidor de vCloud Director debe admitir dos endpoints de SSL diferentes: uno para HTTPS y otro para comunicaciones de proxy de consola.

En el dispositivo de vCloud Director, estos dos endpoints comparten la misma dirección IP o nombre de host, pero utilizan dos puertos distintos: 443 para HTTPS y 8443 para las comunicaciones de proxy de consola. Cada endpoint debe tener su propio certificado SSL. Puede usar el mismo certificado para ambos endpoints, por ejemplo, si utiliza un certificado comodín.

Los certificados de ambos endpoints deben incluir un nombre distintivo X.500 y una extensión de nombre alternativo del firmante X.509.

Si ya cuenta con sus propios archivos de clave privada y de certificado firmado por una entidad de certificación, siga el procedimiento que se describe en [Importar claves privadas y certificados SSL firmados por una entidad de certificación en el dispositivo de vCloud Director](#).

Importante Después de la implementación, el dispositivo de vCloud Director genera certificados autofirmados con un tamaño de clave de 2.048 bits. Debe evaluar los requisitos de seguridad de la instalación antes de elegir un tamaño de clave adecuado. Los tamaños de clave inferiores a 1024 bits ya no se admiten según la publicación especial NIST 800-131A.

En este procedimiento se utiliza como contraseña del almacén de claves la del usuario **raíz**, que se representa como *root_passwd*.

Requisitos previos

Familiarícese con el comando `keytool`. Utilice `keytool` para importar certificados SSL firmados por una entidad de certificación en el dispositivo de vCloud Director. vCloud Director coloca una copia de `keytool` en `opt/vmware/vcloud-director/jre/bin/keytool`.

Procedimiento

- 1 Inicie sesión directamente o utilice SSH en la consola del dispositivo de vCloud Director como **usuario raíz**.
- 2 Según las necesidades del entorno, elija una de las siguientes opciones.

Cuando se implementa el dispositivo de vCloud Director, vCloud Director genera automáticamente certificados autofirmados con un tamaño de clave de 2.048 bits para los servicios HTTPS y de proxy de consola.

- Si desea que la entidad de certificación firme los certificados que se generan con la implementación, vaya al [Paso paso 5](#).
- Si desea generar nuevos certificados con opciones personalizadas, como un tamaño de clave mayor, siga con el [Paso paso 3](#).

- 3 Ejecute el comando para hacer una copia de respaldo del archivo `certificates.ks` existente.

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


- 4 Ejecute el comando para crear pares de claves pública y privada para los servicios HTTPS y de proxy de consola.

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

Al realizar esta acción, el comando crea o actualiza un almacén de claves en `certificates.ks` con la contraseña especificada. Los certificados se crean utilizando los valores predeterminados del comando. Según la configuración de DNS del entorno, el nombre común (Common Name, CN) del emisor se establece como la dirección IP o el FQDN de cada servicio. El certificado utiliza la longitud de clave predeterminada de 2048 bits y caduca un año después de su creación.

Importante Debido a las restricciones de configuración del dispositivo de vCloud Director, debe utilizar la ubicación `/opt/vmware/vcloud-director/certificates.ks` para el almacén de claves de certificados.

Nota Utilice la contraseña **raíz** del dispositivo como contraseña del almacén de claves.

- 5 Cree solicitudes de firma del certificado (Certificate Signing Request, CSR) para los servicios HTTPS y de proxy de consola.

Importante El dispositivo de vCloud Director comparte la misma dirección IP o nombre de host en los servicios HTTPS y de proxy de consola. Por eso, los comandos de creación de CSR deben especificar los mismos DNS y direcciones IP para el argumento de extensión de nombre alternativo del firmante (Subject Alternative Name, SAN).

- a Cree una solicitud de firma del certificado en el archivo `http.csr`.

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

- b Cree una solicitud de firma del certificado en el archivo `consoleproxy.csr`.

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

- 6 Envíe las solicitudes de firma del certificado a la entidad de certificación.

Si la autoridad de certificación le exige especificar un tipo de servidor web, utilice Jakarta Tomcat.

Obtiene los certificados firmados por una entidad de certificación.

- 7 Copie los certificados firmados por una entidad de certificación (incluido el certificado raíz) y los certificados intermedios en el dispositivo de vCloud Director.

8 Ejecute los comandos para importar los certificados firmados en el almacén de claves JCEKS.

- a Importe el certificado raíz de la entidad de certificación del archivo `root.cer` al archivo de almacén de claves `certificates.ks`.

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

- b Si ha recibido certificados intermedios, impórtelos del archivo `intermediate.cer` al archivo de almacén de claves `certificates.ks`.

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

- c Importe el certificado del servicio HTTPS.

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

- d Importe el certificado del servicio de proxy de consola.

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

Los comandos sobrescriben el archivo `certificates.ks` con las versiones de los certificados firmadas por entidades de certificación recientemente adquiridas.

- 9** Para comprobar si los certificados se han importado, ejecute el comando para enumerar el contenido del archivo de almacén de claves.

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

- 10** Ejecute el comando para importar los certificados en la instancia de vCloud Director.

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

- 11** Para que se apliquen los nuevos certificados firmados, reinicie el servicio `vmware-vcd` en el dispositivo de vCloud Director.

```
service vmware-vcd restart
```

Pasos siguientes

- Si utiliza certificados comodín, consulte [Implementar el dispositivo de vCloud Director con certificados comodín firmados para las comunicaciones de proxy de consola y HTTPS](#).
- Si no utiliza certificados comodín, repita este procedimiento en todos los vCloud Director Servers del grupo de servidores.

- Si desea obtener más información sobre cómo sustituir los certificados para la base de datos de PostgreSQL integrada y la interfaz de usuario de administración de dispositivos de vCloud Director, consulte [Reemplazar un certificado autofirmado de interfaz de usuario de administración de dispositivos de vCloud Director y de una instancia integrada de PostgreSQL](#).

Importar claves privadas y certificados SSL firmados por una entidad de certificación en el dispositivo de vCloud Director

Si cuenta con sus propios archivos de clave privada y de certificado firmado por una entidad de certificación, antes de importar los almacenes de claves en el entorno de vCloud Director, cree archivos de almacén de claves en los que importar los certificados y las claves privadas de los servicios HTTPS y de proxy de consola.

Requisitos previos

- Familiarícese con el comando `keytool`. Utilice `keytool` para importar certificados SSL firmados por una entidad de certificación en el dispositivo de vCloud Director. vCloud Director coloca una copia de `keytool` en `opt/vmware/vcloud-director/jre/bin/keytool`.
- Copie en el dispositivo los certificados intermedios, el certificado de CA raíz y los certificados y las claves privadas de los servicios de proxy de consola y HTTPS firmados por una entidad de certificación.

Procedimiento

- 1 Inicie sesión directamente o utilice SSH en la consola del dispositivo de vCloud Director como **usuario raíz**.
- 2 Si dispone de certificados intermedios, ejecute el comando para combinarlos con el certificado raíz firmado por una entidad de certificación y crear una cadena de certificados.

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

- 3 Con la ayuda de OpenSSL, cree archivos de almacén de claves PKCS12 intermedios para los servicios HTTPS y de proxy de consola, con la clave privada, la cadena de certificados y el alias correspondiente. Especifique una contraseña para cada archivo de almacén de claves.

- a Cree el archivo de almacén de claves para el servicio HTTPS.

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

- b Cree el archivo de almacén de claves para el servicio de proxy de consola.

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

- 4 Ejecute el comando para hacer una copia de respaldo del archivo `certificates.ks` existente.

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

- 5 Utilice el comando `keytool` para importar los almacenes de claves PKCS12 en el almacén de claves JCEKS.

- a Importe el almacén de claves PKCS12 para el servicio HTTPS.

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

- b Importe el almacén de claves PKCS12 para el servicio de proxy de consola.

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

- 6 Compruebe que los certificados se han importado correctamente.

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

- 7 Ejecute el comando para importar los certificados firmados en la instancia de vCloud Director.

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

- 8 Para que se apliquen los nuevos certificados firmados por una entidad de certificación, reinicie el servicio `vmware-vcd` en el dispositivo de vCloud Director.

```
service vmware-vcd restart
```

Pasos siguientes

- Si utiliza certificados comodín, consulte [Implementar el dispositivo de vCloud Director con certificados comodín firmados para las comunicaciones de proxy de consola y HTTPS](#).
- Si no utiliza certificados comodín, repita este procedimiento en todas las celdas del dispositivo de vCloud Director del grupo de servidores.
- Si desea obtener más información sobre cómo sustituir los certificados para la base de datos de PostgreSQL integrada y la interfaz de usuario de administración de dispositivos de vCloud Director, consulte [Reemplazar un certificado autofirmado de interfaz de usuario de administración de dispositivos de vCloud Director y de una instancia integrada de PostgreSQL](#).

Reemplazar un certificado autofirmado de interfaz de usuario de administración de dispositivos de vCloud Director y de una instancia integrada de PostgreSQL

De forma predeterminada, la base de datos de PostgreSQL integrada y la interfaz de usuario de administración de dispositivos de vCloud Director comparten un conjunto de certificados SSL autofirmados. Para aumentar la seguridad, puede reemplazar los certificados autofirmados predeterminados por certificados firmados por una entidad de certificación (Certificate Authority, CA).

Cuando se implementa el dispositivo de vCloud Director, se generan certificados autofirmados con un período de validez de 365 días. El dispositivo de vCloud Director utiliza dos conjuntos de certificados SSL. El servicio de vCloud Director utiliza un conjunto de certificados para las comunicaciones de proxy de consola y HTTPS. La base de datos de PostgreSQL integrada y la interfaz de usuario de administración de dispositivos de vCloud Director comparten el otro conjunto de certificados SSL.

Nota El proceso de reemplazo de los certificados de interfaz de usuario de administración de la base de datos y el dispositivo no afecta a los certificados para las comunicaciones de proxy de consola y HTTPS. El reemplazo de uno de los conjuntos de certificados no significa que se deba reemplazar el otro conjunto.

Procedimiento

- 1 Envíe la solicitud de firma del certificado que se encuentra en `/opt/vmware/appliance/etc/ssl/vcd_ova.csr` a la entidad de certificación para firmarla.
- 2 Si va a reemplazar el certificado de la base de datos principal, coloque los demás nodos en modo de mantenimiento para evitar que se pierdan datos.
- 3 Reemplace el certificado con formato PEM existente en `/opt/vmware/appliance/etc/ssl/vcd_ova.crt` por el certificado firmado que obtuvo de la entidad de certificación en el [paso 1](#).
- 4 Para obtener el nuevo certificado, reinicie los servicios de `vpostgres`, `nginx` y `vcd_ova_ui`.

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

```
systemctl restart vpostgres.service
```

- 5 Si va a reemplazar el certificado de la base de datos principal, saque el resto de los nodos de modo de mantenimiento.

Resultados

El nuevo certificado se importará en el almacén de confianza de vCloud Director en las otras celdas de vCloud Director la siguiente vez que se ejecute la función `appliance-sync`. La operación puede durar hasta 60 segundos.

Renovar los certificados del dispositivo de vCloud Director

Cuando se implementa el dispositivo de vCloud Director, se generan certificados autofirmados con un período de validez de 365 días. Si en su entorno hay certificados caducados o que están a punto de hacerlo, puede generar nuevos certificados autofirmados. Debe renovar los certificados para cada celda de vCloud Director de forma individual.

El dispositivo de vCloud Director utiliza dos conjuntos de certificados SSL. El servicio de vCloud Director utiliza un conjunto de certificados para las comunicaciones de proxy de consola y HTTPS. La base de datos de PostgreSQL integrada y la interfaz de usuario de administración de dispositivos de vCloud Director comparten el otro conjunto de certificados SSL.

Puede cambiar ambos conjuntos de certificados autofirmados. Opcionalmente, si utiliza certificados firmados por una entidad de certificación para las comunicaciones de proxy de consola y HTTPS de vCloud Director, puede cambiar únicamente la base de datos de PostgreSQL integrada y el certificado de interfaz de usuario de administración de dispositivos. Los certificados firmados por una entidad de certificación incluyen una cadena de confianza completa que proviene de una entidad de certificación pública reconocida.

Requisitos previos

Si va a renovar el certificado del nodo principal de un clúster de alta disponibilidad de la base de datos, coloque los demás nodos en modo de mantenimiento para evitar que se pierdan datos. Consulte [Administrar una celda](#).

Procedimiento

- 1 Inicie sesión directamente o utilice SSH en el sistema operativo del dispositivo de vCloud Director como **raíz**.
- 2 Para detener los servicios de vCloud Director, ejecute el siguiente comando.

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

- 3 Para generar nuevos certificados autofirmados, ejecute el siguiente comando.

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

Este comando utiliza automáticamente los certificados recién generados para la base de datos integrada de PostgreSQL y la interfaz de usuario de administración de dispositivos. Se reinician los servidores de Nginx y PostgreSQL. El comando genera un nuevo almacén de claves de certificados (`/opt/vmware/vcloud-director/certificates.ks`) con nuevos certificados autofirmados para la comunicación de proxy de consola y HTTPS de vCloud Director, los cuales se utilizan en el [Paso 4](#).

- 4 Si no utiliza certificados firmados por una entidad de certificación, ejecute el comando para importar los certificados autofirmados recién generados en vCloud Director.

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

5 Reinicie el servicio de vCloud Director.

```
service vmware-vcd start
```

Resultados

Los certificados autofirmados renovados se pueden ver en la interfaz de usuario de vCloud Director.

El nuevo certificado de PostgreSQL se importará en el almacén de confianza de vCloud Director en las otras celdas de vCloud Director la siguiente vez que se ejecute la función `appliance-sync`. La operación puede durar hasta 60 segundos.

Pasos siguientes

Si es necesario, se puede reemplazar un certificado autofirmado por un certificado que esté firmado por una entidad de certificación externa o interna.

Configuración del dispositivo de vCloud Director



Puede ver el estado de las celdas de un clúster de HA de la base de datos, realizar una copia de seguridad y restaurar la base de datos integrada, y volver a configurar las opciones del dispositivo.

Después de implementar el dispositivo de vCloud Director, no puede cambiar las direcciones IP de red eth0 y eth1 ni el nombre de host del dispositivo. Si desea que el dispositivo de vCloud Director tenga otras direcciones u otro nombre de host, debe implementar un nuevo dispositivo.

Si debe realizar tareas de mantenimiento en un dispositivo que requiere la desconexión del clúster de alta disponibilidad de la base de datos, para evitar problemas de sincronización, primero debe apagar el dispositivo principal y, a continuación, los dispositivos en espera.

Este capítulo incluye los siguientes temas:

- [Ver el estado de las celdas en un clúster de alta disponibilidad de la base de datos](#)
- [Recuperarse de un error de base de datos principal en un clúster de alta disponibilidad](#)
- [Copia de seguridad y restauración de la base de datos integrada del dispositivo de vCloud Director](#)
- [Configurar el acceso externo a la base de datos de vCloud Director](#)
- [Habilitar o deshabilitar el acceso SSH al dispositivo de vCloud Director](#)
- [Editar la configuración de DNS del dispositivo de vCloud Director](#)
- [Editar las rutas estáticas de las interfaces de red del dispositivo de vCloud Director](#)
- [Scripts de configuración en el dispositivo de vCloud Director](#)
- [Modificar las configuraciones de PostgreSQL en el dispositivo de vCloud Director](#)

Ver el estado de las celdas en un clúster de alta disponibilidad de la base de datos

Para ver el estado de las celdas principales y en espera en un clúster de alta disponibilidad (High Availability, HA) de base de datos de dispositivos, puede iniciar sesión en la interfaz de usuario de administración de dispositivos correspondiente a cualquier celda del clúster de HA de base de datos.

El clúster de HA de base de datos del dispositivo de vCloud Director consta de una celda principal y de dos celdas en espera. Consulte [Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos](#).

Procedimiento

- 1 En un explorador web, desplácese hasta la interfaz de usuario de administración del dispositivo en `https://vcd_ip_address:5480`.
- 2 Inicie sesión como **raíz**.
- 3 Para ver los detalles de las celdas en el clúster de HA de base de datos, haga clic en **Disponibilidad de base de datos de vCD**.

Propiedad	Descripción
Nombre	El nombre DNS de la celda.
Función	Puede ser de tipo principal o en espera. Un clúster de HA de base de datos de dispositivos consta de una celda principal y de dos celdas en espera.
Estado	Puede ser En ejecución, Inaccesible o Con errores. Un asterisco (*) indica el estado de la celda principal.
Siguiendo	El nombre de la celda principal con la que se replica la celda en espera.

Pasos siguientes

Si una celda en espera no está en el estado En ejecución, implemente una nueva celda en espera.

Si la celda principal no está en el estado En ejecución, [Recuperarse de un error de base de datos principal en un clúster de alta disponibilidad](#).

Recuperarse de un error de base de datos principal en un clúster de alta disponibilidad

Si la celda principal no se ejecuta correctamente, para recuperar la base de datos de vCloud Director, se puede promocionar una de las celdas en espera para que se convierta en la nueva celda principal. Después de eso, es necesario implementar una nueva celda en espera.

Requisitos previos

- La celda principal se encuentra en estado inaccesible o con errores.
- Las dos celdas en espera se encuentran en estado en ejecución.

Consulte [Ver el estado de las celdas en un clúster de alta disponibilidad de la base de datos](#).

Procedimiento

- 1 Inicie sesión como **raíz** en la interfaz de usuario de administración de dispositivos de una celda en espera, `https://standby_ip_address:5480`.

- 2 En la columna **Función** de la celda en espera que desea convertir en la nueva celda principal, haga clic en **Promocionar**.

La celda se convierte en la nueva celda principal con un estado en ejecución. La otra celda en espera sigue a la celda principal que se acaba de promocionar.

- 3 Implemente un nuevo dispositivo en espera.

Pasos siguientes

- 1 Elimine el dispositivo principal con errores del grupo de servidores de vCloud Director y del clúster de alta disponibilidad de repmgr. Consulte [Eliminar una celda de nube](#) y [Eliminar del registro una celda principal con errores en un clúster de alta disponibilidad de la base de datos](#).
- 2 Si es necesario, elimine el dispositivo principal con errores.

Copia de seguridad y restauración de la base de datos integrada del dispositivo de vCloud Director

Puede realizar una copia de seguridad de la base de datos PostgreSQL integrada del dispositivo de vCloud Director, lo que le permitirá restaurar el entorno de vCloud Director tras un error.

Realizar una copia de seguridad de la base de datos integrada del dispositivo de vCloud Director

Si el entorno consta de implementaciones de dispositivos de vCloud Director con bases de datos PostgreSQL integradas, puede realizar una copia de seguridad de la base de datos de vCloud Director desde la celda principal. El archivo .tgz resultante se almacena en la ubicación de almacenamiento del servicio de transferencia compartido NFS.

Procedimiento

- 1 Inicie sesión directamente o utilice SSH en la celda principal como **usuario raíz**.
- 2 Desplácese hasta `/opt/vmware/appliance/bin`.
- 3 Ejecute el comando `create-db-backup`.

Resultados

En el almacenamiento del servicio de transferencia compartido de NFS, en el directorio `vcloudapp.nfs_mount.VMware_vCloud_Director/pgdb-backup/`, verá el archivo `db-backup-date_time_format.tgz` que se acaba de crear. El archivo .tgz contiene el archivo de volcado de la base de datos, así como los archivos `global.properties`, `responses.properties`, `certificates` y `proxycertificates` de la celda principal.

Restaurar un entorno de dispositivo de vCloud Director con una configuración de base de datos de alta disponibilidad

Si realizó una copia de seguridad de la base de datos integrada de PostgreSQL correspondiente a un entorno de dispositivo de vCloud Director mediante una configuración de base de datos de alta disponibilidad, puede implementar un nuevo clúster de dispositivos y restaurar en él la base de datos del dispositivo.

Para restaurar una implementación de dispositivo con una configuración de base de datos que no sea de alta disponibilidad, consulte [Restaurar un entorno de dispositivo de vCloud Director sin una configuración de base de datos de alta disponibilidad](#).

El flujo de trabajo de restauración incluye tres etapas principales.

- Copiar el archivo .tar de copia de seguridad de la base de datos integrada a partir del almacenamiento compartido NFS del servicio de transferencia
- Restaurar la base de datos en las celdas principal y en espera de la base de datos integrada.
- Implementar cualquier celda de aplicación requerida.

Requisitos previos

- Compruebe que tiene el archivo .tar de copia de seguridad de la base de datos PostgreSQL integrada. Consulte [Realizar una copia de seguridad de la base de datos integrada del dispositivo de vCloud Director](#).
- Implemente una celda de base de datos principal y dos celdas de base de datos en espera. Consulte la [Capítulo 6 Implementar el dispositivo de vCloud Director](#).
- Si desea que el nuevo clúster de dispositivos use el servidor NFS del entorno existente, cree y exporte un directorio nuevo en el servidor NFS como nuevo punto compartido. No se puede volver a utilizar el punto de montaje existente.

Procedimiento

- 1 En las celdas principal y en espera, inicie sesión como **raíz** y ejecute el comando para detener el servicio de vCloud Director.

```
service vmware-vcd stop
```

- 2 En las celdas principal y en espera, copie el archivo .tar de copia de seguridad en la carpeta /tmp.

Si no hay suficiente espacio libre en la carpeta /tmp, use otra ubicación para almacenar el archivo .tar.

- 3 En las celdas principal y en espera, descomprima el archivo de copia de seguridad en /tmp.

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

En la carpeta /tmp, puede ver los archivos `global.properties`, `responses.properties`, `certificates`, `proxycertificates`, `truststore`, así como el archivo de volcado de la base de datos con el nombre `vcloud_date_time_format`.

Nota El archivo de `truststore` solo está disponible para vCloud Director 9.7.0.1 y versiones posteriores.

- 4 En la celda principal únicamente, inicie sesión como **raíz** en la consola y ejecute los siguientes comandos.

- a Quite la base de datos `vcloud`.

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

- b Ejecute el comando `pg_restore`.

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

- 5 En las celdas principal y en espera, guarde una copia de los archivos de datos de configuración, reemplácelos y vuelva a configurar e iniciar el servicio de vCloud Director.

- a Realice una copia de seguridad de las propiedades, los certificados y los archivos `truststore`.

Los archivos `global.properties`, `responses.properties`, `certificates`, `proxycertificates` y `truststore` están en `/opt/vmware/vcloud-director/etc/`.

Nota El archivo de `truststore` solo está disponible para vCloud Director 9.7.0.1 y versiones posteriores.

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

- b Copie y reemplace las propiedades, los certificados y los archivos `truststore` de los archivos de copia de seguridad que extrajo en el [paso 3](#).

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

Nota El archivo de `truststore` solo está disponible para vCloud Director 9.7.0.1 y versiones posteriores.

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

- c Realice una copia de seguridad del archivo de almacén de claves que se encuentra en `/opt/vmware/vcloud-director/certificates.ks`.

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

- d Ejecute el comando para volver a configurar el servicio de vCloud Director.

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

Donde:

- La opción `--keystore-password` coincide con la contraseña del almacén de claves para los certificados del dispositivo.
- La opción `--database-password` coincide con la contraseña de la base de datos que configuró durante la implementación del dispositivo.
- La opción `--database-host` coincide con la dirección IP de red de `eth1` del dispositivo de la base de datos principal.
- El valor `--primary-ip` coincide con la dirección IP de red de `eth0` de la celda del dispositivo que va a restaurar. Esta no es la dirección IP de la celda de base de datos principal.
- El valor `--console-proxy-ip` coincide con la dirección IP de red de `eth0` del dispositivo que va a restaurar.

Para obtener información sobre cómo solucionar problemas, consulte [Error al volver a configurar el servicio de vCloud Director cuando se realiza una migración al dispositivo de vCloud Director o una restauración en este](#).

- e Ejecute el comando para iniciar el servicio de vCloud Director.

```
service vmware-vcd start
```

Puede supervisar el progreso del inicio de la celda en `/opt/vmware/vcloud-director/logs/cell.log`.

- 6 (opcional) Implemente las celdas de aplicación adicionales. Consulte la [Capítulo 6 Implementar el dispositivo de vCloud Director](#).

- 7 Una vez que todas las celdas del grupo de servidores finalicen el proceso de inicio, compruebe que la restauración del entorno de vCloud Director sea correcta.
 - a Abra la vCloud Director Web Console mediante la dirección IP de red de eth0 de cualquier celda del nuevo grupo de servidores, `https://eth0_IP_new_cell/cloud`.
 - b Inicie sesión en vCloud Director Web Console con las credenciales del **administrador del sistema** existentes.
 - c Compruebe que los recursos de vSphere y de nube estén disponibles en el nuevo entorno.
- 8 Después de la comprobación correcta de la restauración de la base de datos, utilice la vCloud Director Web Console para eliminar las celdas desconectadas que pertenezcan al entorno anterior de vCloud Director.
 - a En la pestaña **Administrar y supervisar**, haga clic en **Celdas de nube**.
 - b Haga clic con el botón secundario en el nombre de una celda y seleccione **Eliminar**.

Restaurar un entorno de dispositivo de vCloud Director sin una configuración de base de datos de alta disponibilidad

Si creó una copia de seguridad de la base de datos integrada de PostgreSQL de un entorno de dispositivo de vCloud Director con una configuración de base de datos que no es de alta disponibilidad, puede implementar un nuevo clúster de dispositivos y restaurar en él la base de datos del dispositivo.

Para restaurar una implementación de dispositivo con una configuración de base de datos de alta disponibilidad, consulte [Restaurar un entorno de dispositivo de vCloud Director con una configuración de base de datos de alta disponibilidad](#).

El flujo de trabajo de restauración incluye tres etapas principales.

- Copiar el archivo .tar de copia de seguridad de la base de datos integrada a partir del almacenamiento compartido NFS del servicio de transferencia
- Restaurar la base de datos en la celda principal de la base de datos integrada.
- Implementar cualquier celda de aplicación requerida.

Requisitos previos

- Compruebe que tiene el archivo .tar de copia de seguridad de la base de datos PostgreSQL integrada. Consulte [Realizar una copia de seguridad de la base de datos integrada del dispositivo de vCloud Director](#).
- Implemente una celda principal de base de datos. Consulte la [Capítulo 6 Implementar el dispositivo de vCloud Director](#).
- Si desea que el nuevo clúster de dispositivos use el servidor NFS del entorno existente, cree y exporte un directorio nuevo en el servidor NFS como nuevo punto compartido. No se puede volver a utilizar el punto de montaje existente.

Procedimiento

- 1 En la celda principal, inicie sesión como **raíz** en la consola y ejecute el comando para detener el servicio de vCloud Director.

```
service vmware-vcd stop
```

- 2 Copie el archivo .tar de copia de seguridad en la carpeta /tmp.

Si no hay suficiente espacio libre en la carpeta /tmp, use otra ubicación para almacenar el archivo .tar.

- 3 Descomprima el archivo de copia de seguridad en /tmp.

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

En la carpeta /tmp, puede ver los archivos `global.properties`, `responses.properties`, `certificates`, `proxycertificates`, `truststore`, así como el archivo de volcado de la base de datos con el nombre `vcloud_date_time_format`.

Nota El archivo de truststore solo está disponible para vCloud Director 9.7.0.1 y versiones posteriores.

- 4 Ejecute los comandos para quitar la base de datos y restaurarla en el nuevo dispositivo.

- a Quite la base de datos vcloud.

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

- b Ejecute el comando `pg_restore`.

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

- 5 En la celda principal, guarde una copia de los archivos de datos de configuración, reemplácelos, vuelva a configurar el servicio de vCloud Director e inícielo.

- a Realice una copia de seguridad de las propiedades, los certificados y los archivos truststore.

Los archivos `global.properties`, `responses.properties`, `certificates`, `proxycertificates` y `truststore` están en `/opt/vmware/vcloud-director/etc/`.

Nota El archivo de truststore solo está disponible para vCloud Director 9.7.0.1 y versiones posteriores.

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

- b Copie y reemplace las propiedades, los certificados y los archivos truststore de los archivos de copia de seguridad que extrajo en el [paso 3](#).

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

Nota El archivo de truststore solo está disponible para vCloud Director 9.7.0.1 y versiones posteriores.

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

- c Realice una copia de seguridad del archivo de almacén de claves que se encuentra en /opt/vmware/vcloud-director/certificates.ks.

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

- d Ejecute el comando para volver a configurar el servicio de vCloud Director.

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

Donde:

- La opción `--keystore-password` coincide con la contraseña del almacén de claves para los certificados del dispositivo.
- La opción `--database-password` coincide con la contraseña de la base de datos que configuró durante la implementación del dispositivo.
- La opción `--database-host` coincide con la dirección IP de red de eth1 del dispositivo de la base de datos principal.
- El valor `--primary-ip` coincide con la dirección IP de red de eth0 de la celda del dispositivo que va a restaurar. Esta no es la dirección IP de la celda de base de datos principal.
- El valor `--console-proxy-ip` coincide con la dirección IP de red de eth0 del dispositivo que va a restaurar.

Para obtener información sobre cómo solucionar problemas, consulte [Error al volver a configurar el servicio de vCloud Director cuando se realiza una migración al dispositivo de vCloud Director o una restauración en este](#).

- e Ejecute el comando para iniciar el servicio de vCloud Director.

```
service vmware-vcd start
```

Puede supervisar el progreso del inicio de la celda en `/opt/vmware/vcloud-director/logs/cell.log`.

- 6 (opcional) Implemente las celdas de aplicación adicionales. Consulte la [Capítulo 6 Implementar el dispositivo de vCloud Director](#).
- 7 Una vez que todas las celdas del grupo de servidores finalicen el proceso de inicio, compruebe que la restauración del entorno de vCloud Director sea correcta.
 - a Abra la vCloud Director Web Console mediante la dirección IP de red de `eth0` de cualquier celda del nuevo grupo de servidores, `https://eth0_IP_new_cell/cloud`.
 - b Inicie sesión en vCloud Director Web Console con las credenciales del **administrador del sistema** existentes.
 - c Compruebe que los recursos de vSphere y de nube estén disponibles en el nuevo entorno.
- 8 Después de la comprobación correcta de la restauración de la base de datos, utilice la vCloud Director Web Console para eliminar las celdas desconectadas que pertenezcan al entorno anterior de vCloud Director.
 - a En la pestaña **Administrar y supervisar**, haga clic en **Celdas de nube**.
 - b Haga clic con el botón secundario en el nombre de una celda y seleccione **Eliminar**.

Configurar el acceso externo a la base de datos de vCloud Director

Es posible habilitar el acceso desde direcciones IP externas determinadas a la base de datos de vCloud Director integrada en el dispositivo principal.

Durante una migración al dispositivo de vCloud Director, o si se planea utilizar una solución de copia de seguridad de base de datos de terceros, se recomienda habilitar el acceso externo a la base de datos de vCloud Director integrada.

Procedimiento

- 1 Inicie sesión directamente o utilice SSH en la celda principal como **usuario raíz**.
- 2 Desplácese hasta el directorio de la base de datos, `/opt/vmware/appliance/etc/pg_hba.d/`.
- 3 Cree un archivo de texto que contenga las entradas de direcciones IP externas de destino similares a:

#TYPE	DATABASE	USER	ADDRESS	METHOD
host	vcloud	vcloud	<i>CIDR_notation</i>	md5

Por ejemplo:

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

Las entradas se anexan al archivo `pg_hba.conf` actualizado dinámicamente, que controla el acceso a la base de datos principal en el clúster de HA.

Habilitar o deshabilitar el acceso SSH al dispositivo de vCloud Director

Durante la implementación del dispositivo, se puede dejar deshabilitado o habilitar el acceso SSH al dispositivo. Después de la implementación, se puede cambiar la configuración de acceso SSH.

El daemon de SSH se ejecuta en el dispositivo para que lo use la función de HA de la base de datos y para los inicios de sesión de **raíz** remotos. Es posible deshabilitar el acceso SSH para el usuario **raíz**. El acceso SSH para la función de HA de la base de datos permanece sin cambios.

Procedimiento

- 1 Si desea realizar cambios temporales en la propiedad de OVF, por ejemplo, para fines de pruebas, cambie la propiedad en vCloud Director.
 - a Inicie sesión directamente o utilice un cliente SSH en la consola del dispositivo de vCloud Director como **raíz**.
 - b Ejecute el script para habilitar o deshabilitar el acceso SSH de **raíz**.
 - Para habilitar el acceso SSH de **raíz**, ejecute el script `/opt/vmware/appliance/bin/enable_root_login.sh`.
 - Para deshabilitar el acceso SSH de **raíz**, ejecute el script `/opt/vmware/appliance/bin/disable_root_login.sh`.
- 2 Si desea realizar cambios permanentes en la propiedad de OVF, utilice la interfaz de usuario de vSphere para establecer el valor de la propiedad `vcloudapp.enable_ssh.VMware_vCloud_Director`.

Nota Debe apagar la máquina virtual para cambiar el valor de la propiedad en vSphere.

- Para habilitar SSH, establezca el valor de `vcloudapp.enable_ssh.VMware_vCloud_Director` en **Verdadero**.
- Para deshabilitar SSH, establezca el valor de `vcloudapp.enable_ssh.VMware_vCloud_Director` en **Falso**.

Editar la configuración de DNS del dispositivo de vCloud Director

Después de la implementación, puede cambiar el servidor o los servidores DNS del dispositivo de vCloud Director.

Importante No se puede editar el nombre de host del dispositivo. Debe implementar un nuevo dispositivo con el nombre de host que desee.

Procedimiento

- 1 Si desea cambiar la configuración de DNS de forma temporal, por ejemplo, para fines de prueba, edite la configuración de DNS en vCloud Director.
 - a Inicie sesión directamente o utilice un cliente SSH en la consola del dispositivo de vCloud Director como **raíz**.
 - b (opcional) Compruebe la configuración de DNS actual mediante la ejecución del siguiente comando:

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

- c Cambie el servidor o los servidores DNS.

Para especificar varios servidores DNS, establezca *DNS_server_IP* como una lista separada por comas sin espacios.

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

- d Para que los cambios surtan efecto, reinicie el servicio VAOS.

```
systemctl restart vaos.service
```

- 2 Si desea cambiar la configuración de DNS de forma permanente, utilice la interfaz de usuario de vSphere para establecer el valor de la propiedad *vami.DNS.VMware_vCloud_Director* en la nueva dirección IP del servidor DNS.

Para especificar varios servidores DNS, escriba una lista separada por comas, sin espacios.

Nota Debe apagar la máquina virtual para cambiar el valor de la propiedad en vSphere.

Editar las rutas estáticas de las interfaces de red del dispositivo de vCloud Director

Puede cambiar las rutas estáticas de las interfaces de red *eth0* y *eth1* después de la implementación inicial de vCloud Director.

Procedimiento

- 1 Si desea cambiar el valor de la ruta estática de forma temporal, por ejemplo, para fines de prueba, edite las rutas estáticas en vCloud Director.

- a Inicie sesión directamente o utilice un cliente SSH en la consola del dispositivo de vCloud Director como **raíz**.
- b (opcional) Compruebe la configuración actual de la ruta estática.

- Para eth0, ejecute el siguiente comando.

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

- Para eth1, ejecute el siguiente comando.

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

- c Cambie el valor de la ruta estática.

Las rutas estáticas deben estar en una lista de especificaciones de rutas separadas por comas. Por ejemplo, para eth0, debe ejecutar lo siguiente:

```
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"
```

- Para eth0, ejecute el siguiente comando.

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

- Para eth1, ejecute el siguiente comando.

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

- d Reinicie el servicio de red en el dispositivo de vCloud Director.

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

- 2 Si desea cambiar el valor de la ruta estática de forma permanente, cambie la propiedad OVF mediante la interfaz de usuario de vSphere.

Las rutas estáticas deben estar en una lista de especificaciones de rutas separadas por comas.

Nota Debe apagar la máquina virtual para cambiar el valor de la propiedad en vSphere.

- Utilice la interfaz de usuario de vSphere para establecer el valor de la propiedad `vcloudnet.routes0.VMware_vCloud_Director` en la nueva cadena de especificación de ruta.
- Utilice la interfaz de usuario de vSphere para establecer el valor de la propiedad `vcloudnet.routes1.VMware_vCloud_Director` en la nueva cadena de especificación de ruta.

Scripts de configuración en el dispositivo de vCloud Director

El dispositivo de vCloud Director contiene scripts de configuración específicos.

Directorio	Descripción
/opt/vmware/appliance/bin/	Los scripts de configuración del dispositivo.
/opt/vmware/appliance/etc/	Los archivos de configuración del dispositivo.
/opt/vmware/appliance/etc/pg_hba.d/	El directorio en el que se pueden añadir entradas personalizadas al archivo <code>pg_hba.conf</code> . Consulte Configurar el acceso externo a la base de datos de vCloud Director .

Modificar las configuraciones de PostgreSQL en el dispositivo de vCloud Director

Puede cambiar las configuraciones de PostgreSQL del dispositivo de vCloud Director mediante el comando `ALTER SYSTEM` de PostgreSQL.

El comando `ALTER SYSTEM` escribe los cambios de la configuración de parámetros en el archivo `postgresql.auto.conf`, el cual tiene prioridad sobre el archivo `postgresql.conf` durante la inicialización de PostgreSQL. Para algunas configuraciones hace falta reiniciar el servicio de PostgreSQL, mientras que otras se configuran dinámicamente y no requieren que se reinicie. No cambie el archivo `postgresql.conf`, ya que esos cambios no se conservan tras el reinicio.

Procedimiento

- 1 Inicie sesión en el sistema operativo del dispositivo principal como **raíz** directamente o mediante un cliente SSH.

- 2 Cambie el usuario a **postgres**.

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

- 3 Utilice el comando `ALTER SYSTEM` de PostgreSQL para cambiar un parámetro.

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

- 4 Repita el [Paso 3](#) para cada parámetro de configuración que desee cambiar.
- 5 Si algunos de los parámetros que desea cambiar requieren que se reinicie el servicio de PostgreSQL, reinicie el proceso `vpostgres`.

```
systemctl restart vpostgres
```

- 6 Si el entorno tiene nodos en espera, copie el archivo `postgresql.auto.conf` en los dispositivos en espera y reinicie el servicio de PostgreSQL si es necesario.

- a Copie el archivo `postgresql.auto.conf` del nodo principal a un nodo en espera.

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

- b Si algunos de los parámetros del archivo `postgresql.auto.conf` que ha copiado requieren que reinicie para hacerse efectivos, reinicie el proceso `vpostgres` en el nodo en espera.

```
systemctl restart vpostgres
```

- c Repita los pasos [6.a](#) y [6.b](#) para cada nodo en espera.

Usar Replication Manager Tool Suite en la configuración de un clúster de alta disponibilidad

9

El paquete de herramientas de código abierto de repmgr forma parte de la base de datos de PostgreSQL integrada del dispositivo de vCloud Director. Puede usar repmgr para configurar, supervisar y controlar la replicación de PostgreSQL y la conmutación por error de la base de datos en el clúster de alta disponibilidad de la base de datos de vCloud Director.

Mediante la interfaz de línea de comandos de repmgr, puede comprobar el estado y los eventos de un nodo o un clúster, registrar un nodo o eliminarlo del registro, promocionar un nodo en espera, intercambiar las funciones de un nodo principal y uno en espera, o seguir un nuevo nodo principal.

Si desea obtener más información sobre la configuración de alta disponibilidad de la base de datos de vCloud Director, consulte [Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos](#).

Para obtener más información sobre repmgr, visite repmgr.org.

Este capítulo incluye los siguientes temas:

- [Comprobar el estado de conectividad de un clúster de alta disponibilidad de la base de datos](#)
- [Comprobar el estado de replicación de un nodo en un clúster de alta disponibilidad de la base de datos](#)
- [Comprobar el estado de un clúster de alta disponibilidad de la base de datos](#)
- [Detectar un nodo principal anterior que vuelve a conectarse en un clúster de alta disponibilidad](#)
- [Cambiar las funciones de la celda principal y una celda en espera en un clúster de alta disponibilidad de la base de datos](#)
- [Eliminar del registro un nodo en espera con errores o inaccesible en un clúster de alta disponibilidad de la base de datos](#)
- [Eliminar del registro una celda principal con errores en un clúster de alta disponibilidad de la base de datos](#)
- [Eliminar del registro una celda en espera en ejecución en un clúster de alta disponibilidad de la base de datos](#)

Comprobar el estado de conectividad de un clúster de alta disponibilidad de la base de datos

Puede utilizar Replication Manager Tool Suite para comprobar la conectividad entre los nodos del clúster de alta disponibilidad de la base de datos.

Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo de cualquiera de las celdas en ejecución del clúster.

- 2 Cambie el usuario a **postgres**.

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

- 3 Compruebe la conectividad del clúster.

- El comando `repmgr cluster matrix` ejecuta el comando `repmgr cluster show` en cada nodo del clúster y presenta el resultado como una matriz.

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

En el siguiente ejemplo, el nodo 1 y el nodo 2 están activos, mientras que el nodo 3 está inactivo. Cada fila corresponde a un servidor y representa el resultado que se obtiene al probar una conexión saliente de ese servidor.

Las tres entradas de la tercera fila están marcadas con un símbolo ? porque el nodo 3 está inactivo y no hay información sobre sus conexiones salientes.

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	x
node 3	3	?	?	?

- El comando `repmgr cluster crosscheck` realiza comprobaciones cruzadas de las conexiones entre cada combinación de nodos y podría proporcionar una mejor descripción general de la conectividad del clúster.

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


En el siguiente ejemplo, el nodo a partir del que se ejecuta el comando `repmgr cluster crosscheck` combina los resultados del sistema de matrices de clústeres con los resultados de los otros nodos y realiza una comprobación cruzada entre los nodos. En este caso, todos los nodos están activos, pero el firewall descarta los paquetes que provienen del nodo 1 y se dirigen al nodo 3. Este es un ejemplo de una partición de red asimétrica, en la que el nodo 1 no puede enviar paquetes al nodo 3.

Name	Id	1	2	3
node 1	1	*	*	x
node 2	2	*	*	*
node 3	3	*	*	*

Pasos siguientes

Para determinar el estado de conectividad general del clúster de alta disponibilidad de la base de datos, ejecute estos comandos en cada nodo y compare los resultados.

Comprobar el estado de replicación de un nodo en un clúster de alta disponibilidad de la base de datos

Puede utilizar Replication Manager Tool Suite y el terminal interactivo de PostgreSQL para comprobar el estado de replicación de nodos individuales en un clúster de alta disponibilidad de la base de datos.

Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo de cualquiera de los nodos en ejecución del clúster.
- 2 Cambie el usuario a **postgres**.

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

- 3 Compruebe el estado de replicación del nodo.

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

Los resultados del sistema proporcionan información sobre el nodo, la versión de PostgreSQL y los detalles de replicación.

- 4 (opcional) Si desea obtener información más detallada, utilice el terminal interactivo de PostgreSQL para comprobar el estado de replicación de los nodos.

El terminal interactivo de PostgreSQL puede proporcionar información en torno a si alguno de los registros recibidos de los nodos en espera está desactualizado en relación con los registros que envió el nodo principal.

- a Conéctese al terminal de `psql`.

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

- b Para expandir la pantalla y facilitar la lectura de los resultados de la consulta, ejecute el comando `set \x`.
- c Ejecute una consulta de estado de replicación según la función del nodo.

Opción	Acción
Ejecute una consulta en el nodo principal.	<code>/opt/vmware/vpostgres/current/bin/psql</code>
Ejecute una consulta en un nodo en espera.	<code>select * from pg_stat_wal_receiver;</code>

Comprobar el estado de un clúster de alta disponibilidad de la base de datos

Para solucionar problemas en el clúster de alta disponibilidad de la base de datos, debe supervisar el estado de los nodos y los eventos del clúster.

Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo de cualquiera de las celdas en ejecución del clúster.
- 2 Cambie el usuario a **postgres**.

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

- 3 Compruebe el estado del clúster.

La columna **Upstream** muestra el nodo principal actual.

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

Los resultados de la consola muestran la información del clúster. En el siguiente ejemplo, no se puede acceder al nodo principal del clúster (el nodo 3).

```

ID | Name      | Role   | Status   | Upstream | Location | Connection string
---+-----+-----+-----+-----+-----+-----
Node 1 | Node name | standby | running | Node 3 name | default | host=host IP address

```

```

user=repmgr dbname=repmgr
Node 2 | Node name | standby |      running      | Node 3 name| default | host=host IP address
user=repmgr dbname=repmgr
Node 3 | Node name | primary | ? unreachable |      | default | host=host IP address
user=repmgr dbname=repmgr

```

En el siguiente ejemplo de resultados del sistema, el nodo 3 es el nodo principal en un clúster en ejecución en buen estado.

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

4 Compruebe el registro de eventos del clúster.

```

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

```

Los resultados del sistema muestran los eventos de creación, clonación y registro del clúster.

Pasos siguientes

Si el estado del nodo principal es `unreachable` o `failed`, debe promocionar un nodo en espera.

Si el estado de un nodo en espera es `unreachable` o `failed`, repare el nodo e inicie el servicio de PostgreSQL si no se está ejecutando.

Detectar un nodo principal anterior que vuelve a conectarse en un clúster de alta disponibilidad

Si se produce un error en un nodo principal del clúster y después se vuelve a conectar cuando se promociona un nodo en espera para que sea el nuevo nodo principal, se pueden producir inexactitudes en los datos de `repmgr`. Puede detectar irregularidades con el comando `repmgr cluster show`.

Ejemplo: Ejecutar `repmgr cluster show` en el nodo principal anterior

En el siguiente ejemplo, al ejecutar el comando `repmgr cluster show` en un nodo principal anterior que vuelve a conectarse, se generan los siguientes resultados del sistema.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Nombre de nodo 1	standby	!running as primary	Nombre de nodo 3	default	host=dirección IP de host user=repmgr dbname=repmgr
Node 2	Nombre de nodo 2	standby	running	Nombre de nodo 3	default	host=dirección

```
IP de host user=repmgr dbname=repmgr
Node 3 | Nombre de nodo 3 | primary | * running | | default | host=dirección IP de
host user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is registered as standby but running as primary
```

En el ejemplo, el nodo 1 es el nodo principal actual del clúster.

Cuando se ejecuta el comando `repmgr cluster show`, el estado `!running as primary` para un nodo en espera indica que se está ejecutando un nodo principal anterior en el clúster. En este caso, debe apagar y eliminar del registro el nodo principal anterior.

Ejemplo: Ejecutar `repmgr cluster show` en el nuevo nodo principal

En el siguiente ejemplo, al ejecutar el comando `repmgr cluster show` en el nuevo nodo principal, se generan los siguientes resultados del sistema.

```

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

En este caso, los datos de `repmgr` son correctos. Indican con precisión que el nodo 1 está en ejecución y que es el nodo principal actual. El mensaje de advertencia sobre el nodo 3, el nodo principal anterior, indica que los datos de `repmgr` sobre ese nodo no son precisos.

Ejemplo: Ejecutar `repmgr cluster show` después de promocionar un nodo en espera sin ejecutar `standby follow` en los otros nodos en espera

En el siguiente ejemplo, se pueden ver los datos de `repmgr` en cada nodo de un clúster en el que se produjo un error en el nodo principal. Se promocionó un nodo en espera de forma manual mediante el comando `repmgr standby promote`, pero sin ejecutar `repmgr standby follow` en los otros nodos en espera.

Cuando se ejecuta `repmgr cluster show` en el nuevo nodo principal, los resultados del sistema representan los datos de `repmgr` correctos, pero ningún nodo en espera sigue al nuevo nodo principal (el nodo 2).

```

ID | Name | Role | Status | Upstream | Location | Connection string
-----+-----+-----+-----+-----+-----+-----
Node 1 | Nombre de nodo 1 | primary | * running | | default | host=dirección IP de host
user=repmgr dbname=repmgr
Node 2 | Nombre de nodo 2 | primary | ! running | | default | host=dirección IP de host
```

```
user=repmgr dbname=repmgr
Node 3 |Nombre de nodo 3| standby | running |Nombre de nodo 1| default | host=dirección IP de
host user=repmgr dbname=repmgr
WARNING: following issues were detected
- node 1(ID: Node 1) is running but the repmgr node record is inactive
```

Tanto el nodo 1 (que es el nodo principal anterior) como el nodo 3 (que es el nodo en espera que sigue al nodo principal anterior) proporcionan datos inexactos de repmgr.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Nombre de nodo 1	primary	* running		default	host=dirección IP de host user=repmgr dbname=repmgr
Node 2	Nombre de nodo 2	standby	! running as primary	Nombre de nodo 1	default	host=dirección IP de host user=repmgr dbname=repmgr
Node 3	Nombre de nodo 3	standby	running	Nombre de nodo 1	default	host=dirección IP de host user=repmgr dbname=repmgr

WARNING: following issues were detected
- node 2(ID: Node 2) is registered as standby but running as primary

Ejemplo: Ejecutar repmgr cluster show en un nodo en espera

Al ejecutar el comando en un nodo en espera que sigue al nodo principal actual, los resultados del sistema se generan con datos de repmgr precisos que son idénticos a los datos del nodo principal actual.

Al ejecutar el comando en un nodo en espera que sigue al nodo principal anterior, se producen resultados del sistema que contienen datos de repmgr imprecisos que son idénticos a los datos del nodo principal anterior.

Entradas de registro

Si un nodo principal anterior en el que se produjeron errores vuelve a conectarse después de promocionar un nodo en espera para que sea el nuevo nodo principal, aparecen las siguientes entradas en el archivo update-repmgr-data.log en todos los nodos con datos de repmgr imprecisos.

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

Cambiar las funciones de la celda principal y una celda en espera en un clúster de alta disponibilidad de la base de datos

Puede usar un comando repmgr para intercambiar las funciones del nodo principal y uno de los nodos en espera del clúster de alta disponibilidad de la base de datos durante un mantenimiento planificado.

Requisitos previos

- Ponga todas las celdas de vCloud Director que forman parte del clúster de alta disponibilidad en modo de mantenimiento.
- Compruebe que todos los nodos del clúster estén conectados y en buen estado.

Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo del nodo en espera que desea promocionar.
- 2 Cambie el usuario a **postgres**.

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

- 3 (opcional) Compruebe que se cumplan los requisitos previos para el intercambio. Para ello, ejecute el comando con la opción **--dry-run**.

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

- 4 Intercambie las funciones de la celda principal y la celda en espera.

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

Resultados

La última línea de los resultados de la consola indica que el intercambio en espera se ha completado correctamente.

Pasos siguientes

- 1 Ejecute el comando **reconfigure-database** para actualizar la dirección IP de la base de datos en todas las celdas de vCloud Director. Consulte [Actualizar las direcciones IP de la base de datos en las celdas de vCloud Director](#).
- 2 Cuando vuelva a configurar las celdas de vCloud Director del grupo de servidores para que apunten a la nueva base de datos principal, saque del modo de mantenimiento todas las celdas de vCloud Director que forman parte del clúster de alta disponibilidad.

Eliminar del registro un nodo en espera con errores o inaccesible en un clúster de alta disponibilidad de la base de datos

En un nodo en ejecución en el clúster, se puede utilizar repmgr para eliminar del registro un nodo en espera con errores o inaccesible.

Nota Para que el nodo principal funcione normalmente, al menos un nodo en espera debe estar siempre en ejecución.

Requisitos previos

Para eliminar del registro un nodo en espera que no está en ejecución, debe proporcionar el identificador del nodo. Para buscar la dirección IP, compruebe el estado del clúster y localice el nodo. En esa fila, utilice el valor de host de la columna Cadena de conexión para identificar la dirección IP del nodo. Consulte la [Comprobar el estado de un clúster de alta disponibilidad de la base de datos](#).

Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo de cualquiera de los nodos en ejecución del clúster.
- 2 Cambie el usuario a **postgres**.

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

- 3 Elimine del registro el nodo con errores o inaccesible.

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

Resultados

Al eliminar el nodo del registro, se elimina la información del nodo de los metadatos de repmgr.

Eliminar del registro una celda principal con errores en un clúster de alta disponibilidad de la base de datos

Si se produce un error en el nodo principal del clúster de alta disponibilidad de la base de datos y se promueve un nuevo nodo principal, se debe eliminar del registro el nodo principal con errores para eliminarlo del clúster y evitar datos de estado del clúster incoherentes.

Requisitos previos

- Para eliminar del registro un nodo principal que no se está ejecutando, debe proporcionar el identificador del nodo. Para buscar la dirección IP, compruebe el estado del clúster y localice el nodo. En esa fila, utilice el valor de host de la columna Cadena de conexión para identificar la dirección IP del nodo. Consulte [Comprobar el estado de un clúster de alta disponibilidad de la base de datos](#).
- Compruebe que el nodo principal con errores esté inactivo y sin ninguno de los siguientes nodos en espera, y promueva un nuevo nodo principal.

Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo de cualquiera de los nodos en ejecución del clúster.
- 2 Cambie el usuario a **postgres**.

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

- 3 (opcional) Para comprobar que se cumplan los requisitos previos para eliminar el nodo del registro, ejecute el comando con la opción **--dry-run**.

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

- 4 Elimine el nodo del registro.

```
/opt/vmware/vpostgres/current/bin/repmgr primary unregister --node-id=identificador del nodo
```

Resultados

La operación elimina el nodo de los metadatos de repmgr.

Eliminar del registro una celda en espera en ejecución en un clúster de alta disponibilidad de la base de datos

Si desea utilizar un nodo en otra función o desea eliminarlo del clúster de alta disponibilidad, debe eliminarlo del registro.

Puede ejecutar este comando durante la operación normal del sistema.

Nota Para que el nodo principal funcione normalmente, al menos un nodo en espera debe estar siempre en ejecución.

Requisitos previos

Para eliminar del registro un nodo en espera, debe proporcionar el identificador del nodo. Para buscar la dirección IP, compruebe el estado del clúster y localice el nodo. En esa fila, utilice el valor de host de la columna Cadena de conexión para identificar la dirección IP del nodo. Consulte [Comprobar el estado de un clúster de alta disponibilidad de la base de datos](#).

Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo de cualquiera de los nodos en ejecución del clúster.
- 2 Cambie el usuario a **postgres**.

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

- 3 Elimine el nodo del registro.

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

Resultados

Al eliminar el nodo del registro, se quita el registro del nodo en espera de la tabla de metadatos interna del paquete de herramientas de repmgr.

Después de instalar vCloud Director o implementar el dispositivo de vCloud Director

10

Después de crear el grupo de servidores de vCloud Director, puede instalar archivos de Microsoft Sysprep y la base de datos de Cassandra. Si utiliza una base de datos PostgreSQL, puede configurar SSL y ajustar algunos parámetros en la base de datos.

Este capítulo incluye los siguientes temas:

- [Instalar archivos de Microsoft Sysprep en los servidores](#)
- [Personalizar endpoints públicos](#)
- [Instalar y configurar un agente AMQP de RabbitMQ](#)
- [Instalar y configurar una base de datos de Cassandra para almacenar datos de métricas históricas](#)
- [Realizar configuraciones adicionales en la base de datos externa de PostgreSQL](#)

Instalar archivos de Microsoft Sysprep en los servidores

Si la nube requiere compatibilidad con la personalización de invitado para determinados sistemas operativos de Microsoft antiguos, debe instalar los archivos de Microsoft Sysprep apropiados en cada miembro del grupo de servidores.

Los archivos de Sysprep solo son necesarios para algunos sistemas operativos de Microsoft más antiguos. Si la nube no necesita admitir la personalización de invitado para estos sistemas operativos, no tendrá que instalar los archivos Sysprep.

Para instalar los archivos binarios de Sysprep, puede copiarlos en una ubicación específica del servidor. Debe copiar los archivos para cada miembro del grupo de servidores.

Requisitos previos

Compruebe que tiene acceso a los archivos binarios de 32 y 64 bits de Sysprep de Windows 2003 y Windows XP.

Procedimiento

- 1 Inicie sesión en el servidor de destino como **raíz**.

- 2 Cambie el directorio a `$VCLLOUD_HOME/guestcustomization/default/windows`.

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

- 3 Cree un directorio denominado `sysprep`.

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

- 4 Para cada sistema operativo invitado que requiera archivos binarios de Sysprep, cree un subdirectorio `$VCLLOUD_HOME/guestcustomization/default/windows/sysprep`.

Los nombres de subdirectorio son específicos de un sistema operativo invitado.

Tabla 10-1. Asignaciones de subdirectorios para archivos de Sysprep

SO invitado	Subdirectorio para crear en <code>\$VCLLOUD_HOME/guestcustomization/default/windows/sysprep</code>
Windows 2003 (32 bits)	svr2003
Windows 2003 (64 bits)	svr2003-64
Windows XP (32 bits)	xp
Windows XP (64 bits)	xp-64

Por ejemplo, utilice el siguiente comando Linux para crear un subdirectorio para almacenar archivos binarios de Sysprep para Windows XP.

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

- 5 Copie los archivos binarios de Sysprep en la ubicación adecuada de cada servidor de vCloud Director en el grupo de servidores.
- 6 Asegúrese de que los archivos Sysprep sean legibles para el usuario `vcld:vcld`.

Utilice el comando `chown` de Linux para ello.

```
[root@cell1 /]# chown -R vcld:vcld $VCLLOUD_HOME/guestcustomization
```

Resultados

Cuando los archivos Sysprep se hayan copiado en todos los miembros del grupo de servidores, podrá realizar una personalización de invitado en las máquinas virtuales de su nube. No tendrá que reiniciar vCloud Director cuando se hayan copiado los archivos de Sysprep.

Personalizar endpoints públicos

Para satisfacer los requisitos de equilibrador de carga o proxy, puede cambiar las direcciones web predeterminadas del endpoint para la consola web de vCloud Director, vCloud API, el portal para tenants y el proxy de la consola.

Si implementó el dispositivo de vCloud Director, debe configurar la dirección de proxy de la consola pública de vCloud Director, ya que el dispositivo utiliza una única dirección IP con el puerto personalizado 8443 para el servicio de proxy de la consola. Consulte el [paso 5](#).

Requisitos previos

Solo el **administrador del sistema** puede personalizar endpoints públicos.

Procedimiento

- 1 Haga clic en la pestaña **Administración** y, en el panel de la izquierda, haga clic en **Direcciones públicas**.

- 2 Seleccione **Personalizar endpoints públicos**.

Al desactivar esta casilla, se vuelven a establecer los valores predeterminados de todos los endpoints, los cuales no aparecen en la página.

- 3 Para personalizar la API de REST de vCloud y las URL de OpenAPI, edite los endpoints de la **API**.

- a Introduzca una URL base HTTP personalizada.

Por ejemplo, si establece la URL base HTTP como **http://vcloud.example.com**, podrá acceder a vCloud API en `http://vcloud.example.com/api` y a vCloud OpenAPI en `http://vcloud.example.com/cloudapi`.

- b Introduzca una URL base de API de REST HTTPS personalizada y haga clic en **Examinar** para cargar los certificados que establecen la cadena de confianza de ese endpoint.

Por ejemplo, si establece la URL base de API de REST HTTPS como **https://vcloud.example.com**, podrá acceder a vCloud API en `https://vcloud.example.com/api` y a vCloud OpenAPI en `https://vcloud.example.com/cloudapi`.

La cadena de certificados debe coincidir con el certificado que utiliza el endpoint del servicio, el cual es el certificado cargado en cada almacén de claves de celdas de vCloud Director con el alias `http` o el certificado VIP del equilibrador de carga en caso de utilizar una terminación SSL. La cadena de certificados debe incluir un certificado de endpoint, certificados intermedios y un certificado raíz con el formato PEM sin una clave privada.

- 4 Para personalizar las URL del portal para tenants de vCloud Director, edite los endpoints del **portal para tenants**.

- Para configurar el portal para tenants de vCloud Director para que use los mismos endpoints y la misma cadena de certificados que se especificó en el [Paso paso 3](#), seleccione **Copiar configuración de URL de API**.

- Para configurar el portal para tenants de vCloud Director para que use endpoints y cadenas de certificados diferentes, realice los siguientes pasos.

- a Anule la selección de **Copiar configuración de URL de API**.

- b Introduzca una URL base HTTP personalizada.

Por ejemplo, si establece la URL base HTTP como **http://vcloud.example.com**, podrá acceder al portal para tenants en **http://vcloud.example.com/tenant/org_name**.

- c Introduzca una URL base de API de REST HTTPS personalizada y haga clic en **Examinar** para cargar los certificados que establecen la cadena de confianza de ese endpoint.

Por ejemplo, si establece la URL base de API de REST HTTPS como **https://vcloud.example.com**, podrá acceder al portal para tenants en **https://vcloud.example.com/tenant/org_name**.

La cadena de certificados debe coincidir con el certificado que utiliza el endpoint del servicio, el cual es el certificado cargado en cada almacén de claves de celdas de vCloud Director con el alias `http` o el certificado VIP del equilibrador de carga en caso de utilizar una terminación SSL. La cadena de certificados debe incluir un certificado de endpoint, certificados intermedios y un certificado raíz con el formato PEM sin una clave privada.

- 5** Para personalizar las URL de vCloud Director Web Console y la dirección de proxy de la consola, edite los endpoints de la **consola web**.

- a Introduzca una URL pública de vCloud Director personalizada para las conexiones HTTP.

La URL debe incluir /cloud.

Por ejemplo, si establece la URL pública de vCloud Director como

http://vcloud.example.com/cloud, podrá acceder a la vCloud Director Web Console en **http://vcloud.example.com/cloud**.

- b Introduzca una URL de API de REST personalizada para conexiones HTTPS y haga clic en **Examinar** para cargar los certificados que establecen la cadena de confianza de ese endpoint.

La URL debe incluir /cloud.

Por ejemplo, si establece la URL base como **https://vcloud.example.com**, podrá acceder a la vCloud Director Web Console en **https://vcloud.example.com/cloud**.

La cadena de certificados debe coincidir con el certificado que utiliza el endpoint del servicio, el cual es el certificado cargado en cada almacén de claves de celdas de vCloud Director con el alias **HTTP** o el certificado VIP del equilibrador de carga en caso de utilizar una terminación SSL. La cadena de certificados debe incluir un certificado de endpoint, certificados intermedios y un certificado raíz con el formato PEM sin una clave privada.

- c Introduzca una dirección de proxy de consola pública de vCloud Director personalizada.

Esta dirección es el nombre de dominio completo (Fully Qualified Domain Name, FQDN) del equilibrador de carga o el servidor de vCloud Director con el número de puerto. El puerto predeterminado es 443.

Importante El dispositivo de vCloud Director utiliza su NIC eth0 con el puerto personalizado 8443 para el servicio de proxy de la consola.

No se admite la terminación SSL de conexiones de proxy de la consola en un equilibrador de carga. El certificado del proxy de consola se carga en cada almacén de claves de celdas de vCloud Director con el alias **consoleproxy**.

Por ejemplo, para una instancia de dispositivo de vCloud Director con el FQDN **vcloud.example.com**, introduzca **vcloud.example.com:8443**.

La consola web de vCloud Director utiliza la dirección de proxy de la consola al abrir una ventana de consola remota en una máquina virtual.

- 6** Para guardar los cambios, haga clic en **Aplicar**.

Instalar y configurar un agente AMQP de RabbitMQ

AMQP, el protocolo de cola de mensajes avanzado, es un estándar abierto para las colas de mensajes que admite mensajería flexible para sistemas corporativos. vCloud Director utiliza el

agente AMQP de RabbitMQ para proporcionar el bus de mensajería utilizado por los servicios de extensión, las extensiones de objeto y las notificaciones.

Procedimiento

- 1 Descargue el servidor de RabbitMQ de <https://www.rabbitmq.com/download.html>.

Consulte la *Notas de la versión de vCloud Director* para obtener una lista de las versiones de RabbitMQ compatibles.

- 2 Siga las instrucciones de instalación de RabbitMQ para instalar RabbitMQ en un host compatible.

Las celdas de vCloud Director deben poder conectar con el servidor RabbitMQ en la red.

- 3 Durante la instalación de RabbitMQ, anote los valores que necesitará para configurar vCloud Director de modo que funcione con esta instalación de RabbitMQ.

- El nombre de dominio completo del host del servidor RabbitMQ, por ejemplo, *amqp.ejemplo.com*.
- Un nombre de usuario y una contraseña válidos para la autenticación con RabbitMQ.
- El puerto en el que el broker escucha los mensajes. El valor predeterminado es 5672.
- El host virtual de RabbitMQ. El valor predeterminado es "/"

Pasos siguientes

El servicio AMQP de vCloud Director envía mensajes sin cifrar AMQP de manera predeterminada. Puede configurar el servicio AMQP para cifrar estos mensajes mediante SSL. También puede configurar el servicio para comprobar el certificado de agente mediante el almacén de confianza de JCEKS predeterminado de Java Runtime Environment en la celda de vCloud Director, por lo general, en `$VCLLOUD_HOME/jre/lib/security/cacerts`.

Para habilitar SSL con el servicio AMQP de vCloud Director:

- 1 En la consola web de vCloud Director, haga clic en la pestaña **Administración** y haga clic en **Extensibilidad**.
- 2 Haga clic en **Extensibilidad** y haga clic en la pestaña **Configuración**.
- 3 En la sección **Configuración de broker AMQP**, seleccione **Utilizar SSL**.
- 4 Active la casilla **Aceptar todos los certificados** o proporcione uno de los siguientes:
 - un nombre de ruta de certificado SSL o
 - un nombre de ruta y contraseña de almacén de confianza de JCEKS

Instalar y configurar una base de datos de Cassandra para almacenar datos de métricas históricas

vCloud Director puede recopilar métricas que ofrecen información actual e histórica sobre el rendimiento y consumo de recursos de las máquinas virtuales que se encuentran en su nube. Los datos de las métricas históricas se almacenan en un clúster de Cassandra.

Cassandra es una base de datos de código abierto que sirve para proporcionar el almacén de respaldo de una solución escalable de alto rendimiento para recopilar datos de series temporales, como las métricas de máquinas virtuales. Si desea que vCloud Director admita la recuperación de métricas históricas de las máquinas virtuales, debe instalar y configurar un clúster de Cassandra, y utilizar `cell-management-tool` para conectar el clúster con vCloud Director. La recuperación de las métricas actuales no requiere software de base de datos opcional.

Requisitos previos

- Verifique que vCloud Director está instalado y ejecutándose antes de configurar el software de base de datos opcional.
- Si aún no está familiarizado con Cassandra, revise el material en <http://cassandra.apache.org/>.
- Consulte la *Notas de la versión de vCloud Director* para obtener una lista de versiones de Cassandra que puede usar como una base de datos de métricas. Puede descargar Cassandra desde <http://cassandra.apache.org/download/>.
- Instalar y configurar el clúster de Cassandra:
 - El clúster de Cassandra debe incluir al menos cuatro máquinas virtuales implementadas en dos hosts o más.
 - Se necesitan dos nodos de inicialización de Cassandra.
 - Habilite el cifrado de cliente a nodo de Cassandra. Consulte <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureSSLIntro.html>.
 - Habilite la autenticación de usuario de Cassandra. Consulte <http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureConfigNativeAuth.html>.
 - Habilite Java Native Access (JNA) versión 3.2.7 o posterior en cada clúster de Cassandra.
 - El cifrado de nodo a nodo de Cassandra es opcional.
 - El uso de SSL con Cassandra es opcional. Si decide no activar SSL para Cassandra, debe establecer el parámetro de configuración `cassandra.use.ssl` como `0` en el archivo `global.properties` en cada celda (`$VCLLOUD_HOME/etc/global.properties`).

Procedimiento

- 1 Use la utilidad `cell-management-tool` para configurar una conexión entre vCloud Director y los nodos del clúster de Cassandra.

En el siguiente comando de ejemplo, *node1-ip*, *node2-ip*, *node3-ip* y *node4-ip* son las direcciones IP de los miembros del clúster de Cassandra. Se utiliza el puerto predeterminado (9042). Los datos de las métricas se conservan durante 15 días.

```
[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 'P055w0rd' --ttl 15
```

Para obtener información sobre el uso de la herramienta de administración de celdas, consulte *Guía del administrador de vCloud Director*.

- 2 (opcional) Si va a actualizar vCloud Director desde la versión 9.1, utilice `cell-management-tool` para configurar la base de datos de métricas y almacenar las métricas resumidas.

Ejecute un comando similar al siguiente ejemplo:

```
[root@cell1 /opt/vmware/vcloud-director/
bin]# ./cell-management-tool cassandra --add-rollup \ --username admin --password 'P055w0rd'
```

- 3 Reinicie cada celda de vCloud Director.

Realizar configuraciones adicionales en la base de datos externa de PostgreSQL

Después de crear el grupo de servidores de vCloud Director, es posible configurar la base de datos externa de PostgreSQL para que solicite conexiones SSL desde las celdas de vCloud Director y ajuste algunos parámetros de base de datos para obtener un rendimiento óptimo.

Las conexiones más seguras requieren un certificado SSL firmado correctamente, que incluye una cadena de confianza completa basada en una entidad de certificación pública reconocida. Como alternativa, puede utilizar un certificado SSL autofirmado o un certificado SSL firmado por una entidad de certificación privada, pero debe importar el certificado al almacén de confianza de vCloud Director.

Para obtener un rendimiento óptimo para la especificación y los requisitos del sistema, puede ajustar la configuración de la base de datos y los parámetros de autovacuum en el archivo de configuración de la base de datos.

Procedimiento

1 Configure conexiones SSL entre vCloud Director y la base de datos de PostgreSQL.

- a Si utiliza un certificado autofirmado o privado para la base de datos externa de PostgreSQL, desde cada celda de vCloud Director, ejecute el comando para importar el certificado de la base de datos al almacén de confianza de vCloud Director.

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

- b Ejecute el comando para habilitar las conexiones SSL entre vCloud Director y PostgreSQL.

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

Puede ejecutar el comando con todas las celdas del grupo de servidores mediante la opción `--private-key-path`.

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

Para obtener más información sobre el uso de la herramienta de administración de celdas, consulte *Guía del administrador de vCloud Director*.

2 Edite la configuración de la base de datos en el archivo `postgresql.conf` para la especificación del sistema.

Por ejemplo, para un sistema con 16 GB de memoria, puede utilizar el siguiente fragmento.

```
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 Edite los parámetros de autovacuum en el archivo `postgresql.conf` según lo requiera.

Para cargas de trabajo de vCloud Director habituales, puede utilizar el siguiente fragmento.

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

El sistema establece un valor de `autovacuum_vacuum_scale_factor` personalizado para la actividad y las tablas de `activity_parameters`.

Pasos siguientes

Si modificó el archivo `postgresql.conf`, debe reiniciar la base de datos.

Actualizar vCloud Director y aplicar revisiones al dispositivo de vCloud Director

11

Puede realizar una actualización orquestada, actualizar vCloud Director manualmente a una nueva versión o aplicar revisiones a las implementaciones del dispositivo de vCloud Director.

Si el grupo de servidores de vCloud Director existente consta de instalaciones de vCloud Director en Linux, puede usar el instalador de vCloud Director para que Linux actualice el entorno. Como alternativa, puede migrar el entorno al dispositivo de vCloud Director 9.7. Consulte [Capítulo 12 Migrar al dispositivo de vCloud Director](#).

Si el grupo de servidores de vCloud Director existente consta de implementaciones de dispositivos de vCloud Director 9.5, solo podrá migrar el entorno al dispositivo de vCloud Director 9.7. El instalador de vCloud Director de Linux se utiliza para actualizar el entorno de existente solo como parte del flujo de trabajo de migración. Consulte [Capítulo 12 Migrar al dispositivo de vCloud Director](#).

Puede [Realizar una actualización orquestada de una instalación de vCloud Director](#) o [Actualizar manualmente una instalación de vCloud Director](#). Con la actualización orquestada, puede ejecutar un solo comando para actualizar todas las celdas en el grupo de servidores y la base de datos. Con la actualización manual, debe actualizar cada celda y la base de datos en secuencia.

A partir de vCloud Director 9.5:

- Las bases de datos de Oracle no son compatibles. Si su instalación de vCloud Director existente utiliza una base de datos de Oracle, consulte [Flujo de trabajo de actualización de una instalación de vCloud Director con una base de datos de Oracle](#).
- No se permite habilitar ni deshabilitar hosts ESXi. Antes de iniciar la actualización, debe habilitar todos los hosts ESXi. Puede colocar los hosts de ESXi en modo de mantenimiento con vSphere Web Client.
- vCloud Director utiliza Java con una compatibilidad mejorada con LDAP. Si utiliza un servidor LDAPS, para evitar errores de inicio de sesión de LDAP, debe comprobar que tiene un certificado generado correctamente. Para obtener información, consulte *Cambios de la versión Java 8* en <https://www.java.com>.

Cuando actualice vCloud Director, la nueva versión deberá ser compatible con los siguientes componentes de la instalación existente:

- El software de base de datos que utiliza actualmente la base de datos de vCloud Director.

Si su instalación de vCloud Director existente utiliza una base de datos de Oracle, consulte [Flujo de trabajo de actualización de una instalación de vCloud Director con una base de datos de Oracle](#).

- La versión de VMware vSphere® en uso.
- La versión de VMware NSX® en uso.

Para obtener información sobre las rutas de actualización y la compatibilidad de vCloud Director con otros productos de VMware y con bases de datos de otros fabricantes, consulte las *matrices de interoperabilidad de productos de VMware* en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php. Si tiene pensado actualizar componentes de NSX o vSphere como parte de la actualización de vCloud Director, deberá actualizarlos tras actualizar vCloud Director ([Capítulo 13 Después de actualizar o migrar vCloud Director](#)).

Después de actualizar al menos un servidor de vCloud Director, puede actualizar la base de datos de vCloud Director. La base de datos almacena información en cuanto al estado de tiempo de ejecución del servidor, incluso el estado de todas las tareas de vCloud Director que esté ejecutando. Para garantizar que no se conserve ninguna información de tarea no válida en la base de datos después de la actualización, debe comprobar que no existan tareas activas en ningún servidor antes de comenzar la actualización.

La versión actualizada también conserva las siguientes funciones, que no se encuentran almacenadas en la base de datos de vCloud Director:

- Los archivos de propiedades locales y globales se copian en la nueva instalación.
- Los archivos de Microsoft Sysprep que se utilizan para la compatibilidad con la personalización de invitado se copian en la nueva instalación.

La actualización requiere suficiente tiempo de inactividad de vCloud Director para actualizar todos los servidores del grupo de servidores y la base de datos. Si utiliza un equilibrador de carga, puede configurarlo para que devuelva un mensaje, como *El sistema está sin conexión debido a la actualización*.

Flujo de trabajo de actualización de una instalación de vCloud Director con una base de datos de Oracle

Antes de actualizar una instalación de vCloud Director que utiliza una base de datos de Oracle, debe migrar la base de datos a PostgreSQL a partir de vCloud Director 9.1.

- 1 Si su versión actual de vCloud Director es anterior a la 9.1, realice la actualización a esta versión.

Para obtener información sobre la actualización de vCloud Director a la versión 9.1, consulte *Guía de instalación, configuración y actualización de vCloud Director 9.1*.

- 2 Si su instalación de vCloud Director tiene la versión 9.1, migre la base de datos de Oracle a una base de datos de PostgreSQL.

Para obtener información sobre la migración a una base de datos de PostgreSQL, consulte la referencia de la herramienta de administración de celdas en la documentación de *Guía del administrador de vCloud Director*.

- 3 Actualice su instalación de vCloud Director a partir de la versión 9.1. Puede realizar los siguientes procedimientos: [Realizar una actualización orquestada de una instalación de vCloud Director](#) o [Actualizar manualmente una instalación de vCloud Director](#).

Aplicar revisiones a la implementación del dispositivo de vCloud Director

Puede aplicar revisiones al dispositivo de vCloud Director para mejorar su funcionalidad o seguridad. Consulte la [Aplicar revisiones a la implementación del dispositivo de vCloud Director](#). Después de aplicar la revisión a cada dispositivo de vCloud Director y de que se complete la actualización de la base de datos, debe reiniciar los servicios de vCloud Director en el grupo de servidores para volver a conectarlo.

Este capítulo incluye los siguientes temas:

- [Realizar una actualización orquestada de una instalación de vCloud Director](#)
- [Actualizar manualmente una instalación de vCloud Director](#)
- [Referencia de la utilidad de actualización de bases de datos](#)
- [Aplicar revisiones a la implementación del dispositivo de vCloud Director](#)

Realizar una actualización orquestada de una instalación de vCloud Director

Para actualizar todas las celdas en el grupo de servidores junto con la base de datos compartida, ejecute el instalador de vCloud Director con la opción `--private-key-path`.

Puede utilizar el instalador de vCloud Director para Linux si desea actualizar un grupos de servidores de vCloud Director que conste de instalaciones de vCloud Director en un sistema operativo Linux compatible. Si el grupo de servidores de vCloud Director consta de implementaciones de dispositivos de vCloud Director 9.5, utilice el instalador de vCloud Director de Linux para actualizar el entorno existente solo como parte del flujo de trabajo de migración. Consulte [Capítulo 12 Migrar al dispositivo de vCloud Director](#).

vCloud Director para Linux se distribuye como archivo ejecutable firmado digitalmente con un nombre con el formato `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, donde `v.v.v` representa la versión de producto y `nnnnnn`, el número de compilación. Por ejemplo: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Con este ejecutable, se instala o actualiza vCloud Director.

Al ejecutar el instalador de vCloud Director con la opción `--private-key-path`, puede agregar otras opciones de comando de la utilidad `upgrade`, por ejemplo, `--maintenance-cell`. Para obtener información acerca de las opciones de la utilidad `upgrade` de la base de datos, consulte [Referencia de la utilidad de actualización de bases de datos](#).

Requisitos previos

- Compruebe que la base de datos de vCloud Director, los componentes de vSphere y los componentes NSX sean compatibles con la nueva versión de vCloud Director.

Importante Si la instalación de vCloud Director existente utiliza una base de datos de Oracle, compruebe que migró hasta una base de datos de PostgreSQL desde vCloud Director 9.1. Consulte [Flujo de trabajo de actualización de una instalación de vCloud Director con una base de datos de Oracle](#).

- Verifique que dispone de credenciales de superusuario en el servidor de destino.
- Si desea que el instalador verifique la firma digital del archivo de instalación, descargue e instale la clave pública de VMware en el servidor de destino. Si ya ha verificado la firma digital del archivo de instalación, no es necesario volver a verificarla durante la instalación. Consulte [Descarga e instalación de la clave pública de VMware](#).
- Verifique que tiene una clave de licencia válida para usar la versión del software de vCloud Director a la que se está actualizando.
- Compruebe que todas las celdas permitan conexiones SSH del superusuario sin una contraseña. Para realizar una comprobación, puede ejecutar el siguiente comando de Linux:

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

En este ejemplo, se establece la identidad como `vcloud`; a continuación, se establece una conexión SSH con la celda de `cell-ip` como raíz, pero no se proporciona la contraseña raíz. Si el usuario `vcloud.vcloud` puede leer la clave privada de `private-key-path` en la celda local y la clave pública correspondiente está presente en el archivo `authorized-keys` para el usuario raíz en `cell-ip`, el comando se ejecutará correctamente.

Nota El programa de instalación de vCloud Director crea el usuario `vcloud`, el grupo `vcloud` y la cuenta `vcloud.vcloud` para su uso como una identidad con la que se ejecutan los procesos de vCloud Director. El usuario `vcloud` no tiene ninguna contraseña.

- Verifique que todos los hosts de ESXi estén habilitados. A partir de vCloud Director 9.5, no se admiten hosts de ESXi deshabilitados.
- Verifique que todos los servidores del grupo de servidores puedan acceder al almacenamiento del servidor de transferencias compartido. Consulte [Preparar el almacenamiento del servidor de transferencia](#).

- Si la instalación de vCloud Director utiliza un servidor LDAPS, para evitar errores de inicio de sesión LDAP tras la actualización, compruebe que tiene un certificado creado correctamente para Java 8 Update 181. Para obtener información, consulte *Cambios de la versión Java 8* en <https://www.java.com>.

Procedimiento

- 1 Inicie sesión en el servidor de destino como **raíz**.

- 2 Descargue el archivo de instalación en el servidor de destino.

Si ha comprado el software en un medio, copie el archivo de instalación en una ubicación que sea accesible para el servidor de destino.

- 3 Verifique que la suma de comprobación de la descarga coincida con la publicada en la página de descargas.

Los valores de las sumas de comprobación MD5 y SHA1 se publican en la página de descargas. Utilice la herramienta adecuada para verificar que la suma de comprobación del archivo de instalación descargado coincida con la que se muestra en la página de descargas. Un comando de Linux con la forma siguiente muestra la suma de comprobación para *installation-file*.

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

El comando devuelve la suma de comprobación del archivo de instalación que debe coincidir con la suma de comprobación MD5 de la página de descargas.

- 4 Asegúrese de que se pueda ejecutar el archivo de instalación.

El archivo de instalación requiere permiso de ejecución. Para asegurarse de que dispone de dicho permiso, abra una ventana de consola, shell o terminal, y ejecute el siguiente comando Linux, donde *archivo-de-instalación* es el nombre de ruta completo del archivo de instalación de vCloud Director.

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

- 5 En una ventana de consola, shell o terminal, ejecute el archivo de instalación con la opción `--private-key-path` y el nombre de ruta de la clave privada que corresponde a la celda de destino.

Puede añadir otras opciones de comando de la utilidad *upgrade* de la base de datos.

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

Nota No se puede ejecutar el archivo de instalación desde un directorio cuya ruta de acceso incluya espacios integrados.

El instalador detecta una versión anterior de vCloud Director y le pide que confirme la actualización.

Si el instalador detecta una versión de vCloud Director que es igual o posterior a la versión del archivo de instalación, muestra un mensaje de error y se cierra.

6 Introduzca **y** y presione Intro para confirmar la actualización.

Resultados

El instalador iniciará el siguiente flujo de trabajo de actualización de varias celdas.

- 1 Comprueba que el host de la celda actual cumpla todos los requisitos.
- 2 Desempaqueta el paquete RPM de vCloud Director.
- 3 Actualiza el software de vCloud Director en la celda actual.
- 4 Actualiza la base de datos de vCloud Director.
- 5 Actualiza el software vCloud Director en cada una de las celdas restantes y, a continuación, reinicia los servicios de vCloud Director en la celda.
- 6 Reinicia los servicios de vCloud Director en la celda actual.

Pasos siguientes

Inicie los servicios de vCloud Director en todas las celdas del grupo de servidores.

Ahora puede [Actualizar cada instancia de NSX Manager que esté asociada con un sistema vCenter Server adjunto](#); a continuación, [Actualizar sistemas vCenter Server, hosts ESXi e instancias de NSX Edge](#).

Actualizar manualmente una instalación de vCloud Director

Puede actualizar una sola celda mediante la ejecución del instalador de vCloud Director sin las opciones del comando. Antes de reiniciar una celda actualizada, debe actualizar el esquema de base de datos. Actualice el esquema de base de datos después de actualizar al menos una celda del grupo de servidores.

Puede utilizar el instalador de vCloud Director para Linux si desea actualizar un grupos de servidores de vCloud Director que conste de instalaciones de vCloud Director en un sistema operativo Linux compatible. Si el grupo de servidores de vCloud Director consta de implementaciones de dispositivos de vCloud Director 9.5, utilice el instalador de vCloud Director de Linux para actualizar el entorno existente solo como parte del flujo de trabajo de migración. Consulte [Capítulo 12 Migrar al dispositivo de vCloud Director](#).

Para una instalación de vCloud Director en varias celdas, en lugar de actualizar manualmente cada celda y la base de datos en secuencia, puede [Realizar una actualización orquestada de una instalación de vCloud Director](#).

Requisitos previos

- Compruebe que la base de datos de vCloud Director, los componentes de vSphere y los componentes NSX sean compatibles con la nueva versión de vCloud Director.

Importante Si la instalación de vCloud Director existente utiliza una base de datos de Oracle, compruebe que migró hasta una base de datos de PostgreSQL desde vCloud Director 9.1. Consulte [Flujo de trabajo de actualización de una instalación de vCloud Director con una base de datos de Oracle](#).

- Verifique que dispone de credenciales de superusuario para los servidores en el grupo de servidores de vCloud Director.
- Si desea que el instalador verifique la firma digital del archivo de instalación, descargue e instale la clave pública de VMware en el servidor de destino. Si ya ha verificado la firma digital del archivo de instalación, no es necesario volver a verificarla durante la instalación. Consulte [Descarga e instalación de la clave pública de VMware](#).
- Verifique que tiene una clave de licencia válida para usar la versión del software de vCloud Director a la que se está actualizando.
- Verifique que todos los hosts de ESXi estén habilitados. A partir de vCloud Director 9.5, no se admiten hosts de ESXi deshabilitados.

Procedimiento

1 [Actualizar una celda de vCloud Director](#)

El instalador de vCloud Director verifica que el servidor de destino cumpla todos los requisitos previos de la actualización y actualiza el software de vCloud Director en el servidor.

2 [Actualización de la base de datos de vCloud Director](#)

Desde un servidor de vCloud Director actualizado, ejecute una herramienta que actualice la base de datos de vCloud Director. No se debe reiniciar ningún servidor de vCloud Director actualizado sin antes actualizar la base de datos compartida.

Pasos siguientes

Después de actualizar todos los servidores de vCloud Director en el grupo de servidores y la base de datos, puede iniciar los servicios de vCloud Director en todas las celdas.

Puede [Actualizar cada instancia de NSX Manager que esté asociada con un sistema vCenter Server adjunto](#), después de lo cual puede [Actualizar sistemas vCenter Server, hosts ESXi e instancias de NSX Edge](#).

Actualizar una celda de vCloud Director

El instalador de vCloud Director verifica que el servidor de destino cumpla todos los requisitos previos de la actualización y actualiza el software de vCloud Director en el servidor.

vCloud Director para Linux se distribuye como archivo ejecutable firmado digitalmente con un nombre con el formato `vmware-vcloud-director-distribution-v.v.v-nnnnnn.bin`, donde *v.v.v* representa la versión de producto y *nnnnnn*, el número de compilación. Por ejemplo: `vmware-vcloud-director-distribution-8.10.0-3698331.bin`. Con este ejecutable, se instala o actualiza vCloud Director.

Para una instalación de vCloud Director en varias celdas, debe ejecutar al instalador de vCloud Director en cada miembro del grupo de servidores de vCloud Director.

Procedimiento

- 1 Inicie sesión en el servidor de destino como **raíz**.

- 2 Descargue el archivo de instalación en el servidor de destino.

Si ha comprado el software en un medio, copie el archivo de instalación en una ubicación que sea accesible para el servidor de destino.

- 3 Verifique que la suma de comprobación de la descarga coincida con la publicada en la página de descargas.

Los valores de las sumas de comprobación MD5 y SHA1 se publican en la página de descargas. Utilice la herramienta adecuada para verificar que la suma de comprobación del archivo de instalación descargado coincida con la que se muestra en la página de descargas. Un comando de Linux con la forma siguiente muestra la suma de comprobación para *installation-file*.

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

El comando devuelve la suma de comprobación del archivo de instalación que debe coincidir con la suma de comprobación MD5 de la página de descargas.

- 4 Asegúrese de que se pueda ejecutar el archivo de instalación.

El archivo de instalación requiere permiso de ejecución. Para asegurarse de que dispone de dicho permiso, abra una ventana de consola, shell o terminal, y ejecute el siguiente comando Linux, donde *archivo-de-instalación* es el nombre de ruta completo del archivo de instalación de vCloud Director.

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

- 5 Ejecute el archivo de instalación.

Para ejecutar el archivo de instalación, introduzca el nombre de ruta completo; por ejemplo:

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

El archivo incluye un script de instalación y un paquete RPM integrado.

Nota No se puede ejecutar el archivo de instalación desde un directorio cuya ruta de acceso incluya espacios integrados.

Si el instalador detecta una versión de vCloud Director que es igual o posterior a la versión del archivo de instalación, muestra un mensaje de error y se cierra.

Si el instalador detecta una versión anterior de vCloud Director, le solicita que confirme la actualización.

6 Introduzca **y** y presione Intro para confirmar la actualización.

El instalador inicia el siguiente flujo de trabajo de actualización.

- a Comprueba que el host cumpla con todos los requisitos.
- b Desempaqueta el paquete RPM de vCloud Director.
- c Una vez completados todos los trabajos activos de vCloud Director en la celda, detiene los servicios de vCloud Director en el servidor y actualiza el software de vCloud Director instalado.

Si no instaló la clave pública de VMware en el servidor de destino, el instalador muestra una advertencia con el siguiente formato:

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

Al modificar el archivo `global.properties` existente en el servidor de destino, el instalador muestra una advertencia con el siguiente formato:

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

Nota Si actualizó previamente el archivo `global.properties`, puede recuperar los cambios desde `global.properties.rpmnew`.

7 (opcional) Actualice las propiedades de registro.

Después de una actualización, las nuevas propiedades de registro se escriben en el archivo `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew`.

Opción	Acción
Si no ha cambiado las propiedades de registro existentes	Copie este archivo en <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> .
Si ha cambiado las propiedades de registro	Para conservar los cambios, combine <code>/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew</code> con el archivo <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> existente.

Resultados

Una vez finalizada la actualización de vCloud Director, el instalador muestra un mensaje con información sobre la ubicación de los archivos de configuración anteriores. A continuación, el instalador le solicita que ejecute la herramienta de actualización de bases de datos.

Pasos siguientes

Si todavía no la actualizó, puede actualizar la base de datos de vCloud Director.

Repita este procedimiento en cada celda de vCloud Director en el grupo de servidores.

Importante No inicie los servicios de vCloud Director hasta que se actualicen todas las celdas del grupo de servidores y la base de datos.

Actualización de la base de datos de vCloud Director

Desde un servidor de vCloud Director actualizado, ejecute una herramienta que actualice la base de datos de vCloud Director. No se debe reiniciar ningún servidor de vCloud Director actualizado sin antes actualizar la base de datos compartida.

La información en cuanto a todas las tareas que estén en ejecución y las recientemente completadas se almacenan en la base de datos de vCloud Director. Como la actualización de la base de datos invalida la información de la tarea, la utilidad de actualización de bases de datos verifica que no haya tareas en ejecución cuando se inicia el proceso de actualización.

Todas las celdas de un grupo de servidores de vCloud Director comparten la misma base de datos. Independientemente de la cantidad de celdas que se actualicen, la base de datos se actualiza una sola vez. Una vez actualizada la base de datos, las celdas de vCloud Director que no se actualizan no pueden conectarse a la base de datos. Es necesario actualizar todas las celdas para que se conecten a la base de datos actualizada.

Requisitos previos

- Cree una copia de seguridad de la base de datos existente. Utilice los procedimientos que el proveedor del software de base de datos recomienda.
- Compruebe que se hayan detenido todas las celdas de vCloud Director en el grupo de servidores. Las celdas actualizadas se detienen durante el proceso de actualización. Si existen servidores de vCloud Director no actualizados todavía, puede utilizar la herramienta de administración de celdas para poner en modo de inactividad y apagar los servicios. Para obtener información sobre la administración de una celda mediante la herramienta de administración de celdas, consulte *Guía del administrador de vCloud Director*.
- Si la instalación de vCloud Director utiliza una base de datos de Oracle, realice una migración a una base de datos de PostgreSQL. Para obtener información sobre la migración a una base de datos de PostgreSQL, consulte la referencia de la herramienta de administración de celdas en *Guía del administrador de vCloud Director*.
- Revise [Referencia de la utilidad de actualización de bases de datos](#). Las opciones y los argumentos no son obligatorios.

Procedimiento

- 1 Ejecute la utilidad `upgrade` de la base de datos con o sin opciones.

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

Si la utilidad de actualización de bases de datos detecta una versión de NSX Manager no compatible, la utilidad muestra un mensaje de advertencia y cancela la actualización.

- 2 En el aviso, introduzca **y** y presione Intro para confirmar la actualización de la base de datos.
- 3 En el aviso, introduzca **y** y presione Intro para confirmar que se creó una copia de seguridad de la base de datos.

Si utilizó la opción `--backup-completed`, la utilidad omite este aviso.

- 4 Si la utilidad detecta una celda activa, en el aviso para continuar, introduzca **n** para salir del shell. A continuación, compruebe que no haya celdas en ejecución y vuelva a intentar la actualización desde el [Paso paso 1](#).

Resultados

La herramienta de actualización de base de datos se ejecuta y muestra mensajes del progreso. Al finalizar la actualización, se le pedirá que inicie el servicio de vCloud Director en el servidor actual.

Pasos siguientes

Introduzca **y** y presione Intro o inicie el servicio en otro momento mediante el comando `service vmware-vcd start`.

Puede iniciar los servicios de los servidores de vCloud Director actualizados.

Puede actualizar el resto de los miembros de vCloud Director en el grupo de servidores e iniciar sus servicios. Consulte [Actualizar una celda de vCloud Director](#).

Referencia de la utilidad de actualización de bases de datos

Al ejecutar la utilidad `upgrade`, debe proporcionar la información de configuración en la línea de comandos como argumentos y opciones.

Tabla 11-1. Argumentos y opciones de la utilidad de actualización de bases de datos

Opción	Argumento	Descripción
--backup-completed	Ninguno	Especifica que se ha completado una copia de seguridad de vCloud Director. Cuando se incluye esta opción, la utilidad de actualización no solicita que se cree una copia de seguridad de la base de datos.
--ceip-user	El nombre de usuario de la cuenta de servicio del CEIP.	Si ya existe un usuario con este nombre en la organización del sistema, se producirá un error en la actualización. Predeterminado: phone-home-system-account.
--enable-ceip	<p>Elija uno:</p> <ul style="list-style-type: none"> ■ true ■ false 	<p>Especifica si esta instalación participa en el Programa de mejora de la experiencia del cliente (CEIP) de VMware. El valor predeterminado es true si no se lo proporciona y no está configurado en false en la configuración actual. El Programa de mejora de la experiencia del cliente (CEIP) de VMware proporciona información adicional respecto de los datos recopilados a través de él y los objetivos para los que VMware los usa se establecen en el Centro de Seguridad y Confianza, en http://www.vmware.com/trustvmware/ceip.html. En cualquier momento, puede usar la herramienta de administración de celdas para unirse o abandonar el CEIP de VMware para este producto. Consulte "Referencia de la herramienta de administración de celdas" en la <i>Guía del administrador de vCloud Director</i>.</p>

Tabla 11-1. Argumentos y opciones de la utilidad de actualización de bases de datos (continuación)

Opción	Argumento	Descripción
--installer-path	El nombre de ruta completo al archivo de instalación de vCloud Director. El archivo de instalación y el directorio en el que se almacena deben ser legibles para el usuario vcloud.vcloud.	Este producto forma parte del Programa de mejora de la experiencia del cliente (Customer Experience Improvement Program, CEIP) de VMware. En el Centro de Seguridad y Confianza, en http://www.vmware.com/trustvmware/ceip.html , hay información acerca de los datos recopilados a través del CEIP y los fines para los cuales VMware los utiliza. En cualquier momento, puede usar la herramienta de administración de celdas para unirse o abandonar el CEIP de VMware para este producto. Consulte la referencia a la herramienta de administración de celdas en la <i>Guía del administrador de vCloud Director</i> . Requiere la opción --private-key-path .
--maintenance-cell	Dirección IP	La dirección IP de una celda para que la utilidad de actualización se ejecute en modo de mantenimiento durante la actualización. Esta celda pasará al modo de mantenimiento antes de que se desconecte el resto de celdas, y permanecerá en el modo de mantenimiento mientras se actualizan las demás celdas. Después de haber actualizado las demás celdas, y de que se haya reiniciado al menos una de ellas, esta celda se desconectará y se actualizará. Requiere la opción --private-key-path .
--multisite-user	El nombre de usuario para la cuenta del sistema de varios sitios.	Esta cuenta es utilizada por la característica vCloud Director de varios sitios. Si ya existe un usuario con este nombre en la organización del sistema, se producirá un error en la actualización. Predeterminado: multisite-system-account.

Tabla 11-1. Argumentos y opciones de la utilidad de actualización de bases de datos (continuación)

Opción	Argumento	Descripción
--private-key-path	nombre de ruta	Ruta de acceso completa a la clave privada de la celda. Cuando se utiliza esta opción, todas las celdas del grupo de servidores se desconectarán, se actualizarán y se reiniciarán tras la actualización de la base de datos. Consulte Realizar una actualización orquestada de una instalación de vCloud Director para obtener más información acerca de este flujo de trabajo de actualización.
--unattended-upgrade	Ninguno	Especifica una actualización sin supervisión.

Si utiliza la opción `--private-key-path`, todas las celdas se deben configurar para permitir las conexiones ssh del superusuario sin una contraseña. Puede utilizar una línea de comandos de Linux como la que se muestra a continuación para comprobar esto. En este ejemplo, se establece la identidad como `vcloud`; a continuación, se establece una conexión ssh con la celda de `cell-ip` como `root`, pero no se proporciona la contraseña raíz.

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

Si el usuario `vcloud.vcloud` puede leer la clave privada de `private-key-path` de la celda local, y la clave pública correspondiente se ha agregado al archivo `authorized-keys` para el usuario raíz en `cell-ip`, el comando se ejecutará correctamente.

Nota El programa de instalación de vCloud Director crea el usuario `vcloud`, el grupo `vcloud` y la cuenta `vcloud.vcloud` para su uso como una identidad con la que se ejecutan los procesos de vCloud Director. El usuario `vcloud` no tiene ninguna contraseña.

Aplicar revisiones a la implementación del dispositivo de vCloud Director

Puede actualizar el dispositivo de vCloud Director con revisiones que podrían estar relacionadas con las mejoras de seguridad y funcionalidad del producto.

Durante la revisión de la implementación del dispositivo de vCloud Director, el servicio de vCloud Director deja de funcionar y se puede esperar que exista un periodo de inactividad. Este periodo depende del tiempo que se necesite para aplicar la revisión en cada dispositivo de vCloud Director y ejecutar el script de actualización de la base de datos de vCloud Director. La cantidad

de celdas en funcionamiento en el grupo de servidores de vCloud Director se reduce hasta que detenga el servicio de vCloud Director en el último dispositivo de vCloud Director. Un equilibrador de carga configurado correctamente delante de los endpoints HTTP de vCloud Director debería dejar de enrutar el tráfico a las celdas que están detenidas.

Después de aplicar la revisión a cada dispositivo de vCloud Director y de que se complete la actualización de la base de datos, debe reiniciar los servicios de vCloud Director en el grupo de servidores para volver a conectarlo.

Procedimiento

- 1 En un navegador web, inicie sesión en la interfaz de usuario de administración de dispositivos de una instancia del dispositivo de vCloud Director para identificar el dispositivo principal, `https://dirección_IP_de_dispositivo:5480`.

Anote el nombre del dispositivo principal. Debe usarlo cuando actualice la base de datos.

- 2 Descargue el paquete de actualización en un dispositivo.

vCloud Director se distribuye como un archivo ejecutable con un nombre del tipo `VMware_vCloud_Director_v.v.v.v-nnnnnnnn_update.tar.gz`, donde *v.v.v.v* representa la versión de producto y *nnnnnnnn* representa el número de compilación. Por ejemplo, `VMware_vCloud_Director_9.7.0.4248-13560441_update.tar.gz`.

- 3 Cree el directorio `local-update-package` en el que se extraerá el paquete de actualización.

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

- 4 Extraiga el paquete de actualización en el directorio que acaba de crear.

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

- 5 Establezca el directorio `local-update-package` como el repositorio de actualización.

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

- 6 Busque actualizaciones para comprobar que el repositorio se estableció correctamente.

```
vamicli update --check
```

La versión de la revisión aparece como una actualización disponible.

- 7 Ejecute el siguiente comando para apagar vCloud Director:

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <nombre de usuario del administrador>
cell --shutdown
```

- 8 En el dispositivo principal, realice una copia de seguridad de la base de datos integrada del dispositivo de vCloud Director.

Nota Si desea actualizar desde vCloud Director 9.7.0.1 a una versión posterior, cree de forma manual una copia de seguridad del archivo de almacén de confianza que se encuentra en `/opt/vmware/vcloud-director/etc/truststore`.

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

- 9 Aplique la revisión disponible.

```
vamcli update --install latest
```

- 10 En cada dispositivo, repita el proceso desde el [Paso 2](#) hasta el [Paso 7](#) y realice también el [Paso 9](#).
- 11 En cualquier dispositivo, ejecute el script de actualización de la base de datos de vCloud Director.

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

- 12 Inicie los servicios de vCloud Director en cada dispositivo.

```
service vmware-vcd start
```

Migrar al dispositivo de vCloud Director

12

A partir de la versión 9.7, el dispositivo de vCloud Director incluye una base de datos de PostgreSQL integrada con una función de alta disponibilidad. Puede migrar el entorno de vCloud Director existente de una versión anterior a un entorno de vCloud Director que conste de implementaciones de dispositivos de vCloud Director 9.7.

Puede migrar un entorno de vCloud Director que conste de instalaciones de vCloud Director en Linux o implementaciones de dispositivos de vCloud Director. Puede migrar un entorno de vCloud Director que utilice una base de datos Microsoft SQL externa o una base de datos PostgreSQL externa.

Si el entorno de vCloud Director utiliza una base de datos Oracle externa, antes de migrar al dispositivo de vCloud Director, debe migrar la base de datos a PostgreSQL desde la versión 9.1 de vCloud Director. Para obtener información sobre el flujo de trabajo para actualizar una instalación de vCloud Director con una base de datos Oracle, consulte [Capítulo 11 Actualizar vCloud Director y aplicar revisiones al dispositivo de vCloud Director](#).

Este capítulo incluye los siguientes temas:

- [Migrar vCloud Director con una base de datos Microsoft SQL externa al dispositivo de vCloud Director](#)
- [Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director](#)

Migrar vCloud Director con una base de datos Microsoft SQL externa al dispositivo de vCloud Director

Si el entorno actual de vCloud Director de una versión anterior utiliza una base de datos Microsoft SQL externa, puede migrarlo a un nuevo entorno de vCloud Director que conste de implementaciones de dispositivos de vCloud Director 9.7. El entorno de vCloud Director actual puede constar de instalaciones de vCloud Director en Linux o implementaciones de dispositivos de vCloud Director. El nuevo entorno de vCloud Director puede utilizar las bases de datos PostgreSQL integradas del dispositivo en modo de alta disponibilidad.

El flujo de trabajo de migración incluye cuatro etapas principales.

- Crear el nuevo grupo de servidores de vCloud Director mediante la implementación de una o varias instancias del dispositivo de vCloud Director 9.7

- Actualizar el entorno de vCloud Director existente
- Migrar la instancia externa a la base de datos integrada
- Copiar los datos del servicio de transferencia compartido y los datos de certificado

Procedimiento

- 1 Actualice su entorno de vCloud Director actual a la versión 9.7 y actualice el esquema de base de datos de origen.

Consulte [Capítulo 11 Actualizar vCloud Director y aplicar revisiones al dispositivo de vCloud Director](#).

- 2 Compruebe que el reinicio de vCloud Director del origen de migración sea correcto.
- 3 Si desea que el nuevo entorno de vCloud Director use las direcciones IP del entorno existente, cambie las direcciones IP de las celdas existentes a por direcciones IP temporales.
- 4 Si desea que el nuevo entorno de vCloud Director use el servidor NFS del entorno existente, cree y exporte un directorio nuevo en este servidor NFS como nuevo punto de montaje NFS compartido.

No puede reutilizar el punto de montaje existente porque los identificadores de usuario y grupo (UID/GID) de los usuarios del antiguo NFS podrían no coincidir con los identificadores de usuario y grupo en el nuevo NFS.

- 5 Cree el nuevo grupo de servidores mediante la implementación de una o varias instancias del dispositivo de vCloud Director 9.7.
 - Si desea utilizar la función de alta disponibilidad de la base de datos, implemente una celda principal y dos celdas en espera y, de forma opcional, una o varias celdas de aplicación de vCD.
 - Si cambió las direcciones IP de las celdas existentes por direcciones IP temporales, puede usar las direcciones IP originales para las nuevas celdas.
 - Si exportó una nueva ruta de acceso en el servidor NFS existente, puede utilizar este nuevo punto de montaje compartido para el nuevo entorno.

Consulte [Capítulo 6 Implementar el dispositivo de vCloud Director](#).

- 6 En cada celda existente y en cada celda recién implementada, ejecute el comando para detener el servicio de vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <nombre de usuario del administrador>  
cell --shutdown
```

- 7 Elija una de las celdas existentes para que sirva como origen de migración.

El origen de migración debe tener acceso a la dirección IP de red de eth1 de la celda principal recién implementada.

- 8 En la nueva celda principal, habilite el acceso a la base de datos integrada desde el origen de migración.

Consulte [Configurar el acceso externo a la base de datos de vCloud Director](#).

- 9 En el origen de migración, ejecute la herramienta de administración de celdas para migrar la base de datos externa a la base de datos integrada en la nueva celda principal.

La base de datos integrada utiliza la dirección IP de red de eth1 del dispositivo.

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

Para obtener información sobre el uso de la herramienta de administración de celdas, consulte *Guía del administrador de vCloud Director*.

- 10 En cada celda recién implementada, realice una copia de seguridad de los datos de configuración y reemplácelos; a continuación, vuelva a configurar e iniciar el servicio de vCloud Director.
 - a Realice una copia de seguridad de las propiedades y los archivos de certificado, y copie y reemplace dichos archivos del origen de migración.

Los archivos `global.properties`, `responses.properties`, `certificates` y `proxycertificates` están en `/opt/vmware/vcloud-director/etc/`.

Importante Si va a migrar a la versión 9.7.0.1 de vCloud Director o una versión posterior, también debe copiar y reemplazar el archivo `truststore` del origen de migración, así como realizar una copia de seguridad de este archivo, junto con el resto de los archivos.

- b Realice una copia de seguridad del archivo de almacén de claves que se encuentra en `/opt/vmware/vcloud-director/certificates.ks`.

No copie ni reemplace con el archivo de almacén de claves del origen de migración.

- c Ejecute el comando para volver a configurar el servicio de vCloud Director.

```
/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
```

Donde:

- El valor `--keystore-password` coincide con la contraseña **raíz** inicial del dispositivo.
- El valor `--database-password` coincide con la contraseña de la base de datos que configuró durante la implementación del dispositivo.

- El valor `--database-host` coincide con la dirección IP de red de eth1 del dispositivo principal.
- El valor `--keystore` es la ruta de acceso al archivo `certificates.ks` del que creó una copia de seguridad en el paso 10.b.
- El valor `--primary-ip` coincide con la dirección IP de red de eth0 del dispositivo.
- El valor `--console-proxy-ip` coincide con la dirección IP de red de eth0 del dispositivo.

Para obtener información sobre cómo solucionar problemas, consulte [Error al volver a configurar el servicio de vCloud Director cuando se realiza una migración al dispositivo de vCloud Director o una restauración en este](#).

- d Ejecute el comando para iniciar el servicio de vCloud Director.

```
service vmware-vcd start
```

Puede supervisar el progreso del inicio de la celda en `/opt/vmware/vcloud-director/logs/cell.log`.

- 11 Una vez que todas las celdas del nuevo grupo de servidores finalicen el proceso de inicio, compruebe que la migración del entorno de vCloud Director sea correcta.
 - a Abra la vCloud Director Web Console mediante la dirección IP de red de eth0 de cualquier celda del nuevo grupo de servidores, `https://eth0_IP_new_cell/cloud`.
 - b Inicie sesión en vCloud Director Web Console con las credenciales del **administrador del sistema** existentes.
 - c Compruebe que los recursos de vSphere y de nube estén disponibles en el nuevo entorno.
- 12 Después de la comprobación correcta de la migración de vCloud Director, utilice la vCloud Director Web Console para eliminar las celdas desconectadas que pertenezcan al entorno anterior de vCloud Director.
 - a En la pestaña **Administrar y supervisar**, haga clic en **Celdas de nube**.
 - b Haga clic con el botón secundario en el nombre de una celda y seleccione **Eliminar**.

Puede implementar el dispositivo de vCloud Director para agregar miembros al grupo de servidores del entorno migrado.

Qué hacer a continuación

El nuevo entorno del dispositivo de vCloud Director migrado utiliza certificados autofirmados. Para usar los certificados firmados correctamente del entorno anterior, en cada celda del nuevo entorno, siga estos pasos:

- 1 Copie y reemplace el archivo de almacén de claves de la celda anterior en `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.

- 2 Ejecute el comando de la herramienta de administración de celdas para reemplazar los certificados.

Asegúrese de que vcloud.vcloud sea el propietario de este archivo.

```
/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 Reinicie el servicio de vCloud Director.

```
service vmware-vcd restart
```

Si agrega nuevos miembros a este grupo de servidores, las nuevas celdas del dispositivo se implementarán con estos certificados firmados correctamente.

Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director

Si el entorno actual de vCloud Director de una versión anterior utiliza una base de datos PostgreSQL externa, puede migrarlo a un nuevo entorno de vCloud Director que conste de implementaciones de dispositivos de vCloud Director 9.7. El entorno de vCloud Director actual puede constar de instalaciones de vCloud Director en Linux o implementaciones de dispositivos de vCloud Director. El nuevo entorno de vCloud Director puede utilizar las bases de datos PostgreSQL integradas del dispositivo en modo de alta disponibilidad.

El flujo de trabajo de migración incluye cuatro etapas principales.

- Actualizar el entorno de vCloud Director existente
- Crear el nuevo grupo de servidores de vCloud Director mediante la implementación de una o varias instancias del dispositivo de vCloud Director 9.7
- Migrar la instancia externa a la base de datos integrada
- Copiar los datos del servicio de transferencia compartido y los datos de certificado

Procedimiento

- 1 Si la base de datos PostgreSQL externa actual tiene la versión 9.x, actualícela a la versión 10.
- 2 Actualice el entorno de vCloud Director actual a la versión 9.7.

Consulte [Capítulo 11 Actualizar vCloud Director y aplicar revisiones al dispositivo de vCloud Director](#).

- 3 Compruebe que el reinicio de vCloud Director del origen de migración sea correcto.

- 4 En cada celda del entorno de vCloud Director actualizado, ejecute el comando para detener el servicio de vCloud Director.

```
/opt/vmware/vcloud-director/bin/cell-management-tool -u <nombre de usuario del administrador>
cell --shutdown
```

- 5 En la base de datos PostgreSQL externa, realice una copia de seguridad de la base de datos actual.

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

Si no hay suficiente espacio libre en la carpeta /tmp, use otra ubicación para almacenar el archivo de volcado.

- 6 Si el propietario y el nombre de la base de datos son diferentes de vcloud, anote el nombre de usuario y el nombre de la base de datos.

Debe crear este usuario en el nuevo entorno y cambiar el nombre de la base de datos en el paso 13.

- 7 Si desea que el nuevo entorno de vCloud Director utilice las direcciones IP del entorno existente, debe copiar las propiedades y los archivos de certificado en una ubicación en la base de datos de PostgreSQL externa y desconecte las celdas.
 - a Copie los archivos `global.properties`, `responses.properties`, `certificates` y `proxycertificates` que se encuentran en `/opt/vmware/vcloud-director/etc/` en `/tmp` o en cualquier otra ubicación que prefiera de la base de datos de PostgreSQL externa.
 - b Desconecte las celdas del entorno existente.

- 8 Si desea que el nuevo entorno de vCloud Director use el servidor NFS del entorno existente, cree y exporte un directorio nuevo en este servidor NFS como nuevo punto de montaje NFS compartido.

No puede reutilizar el punto de montaje existente porque los identificadores de usuario y grupo (UID/GID) de los usuarios del antiguo NFS podrían no coincidir con los identificadores de usuario y grupo en el nuevo NFS.

- 9 Cree el nuevo grupo de servidores mediante la implementación de una o varias instancias del dispositivo de vCloud Director 9.7.
 - Si desea utilizar la función de alta disponibilidad de la base de datos, implemente una celda principal y dos celdas en espera y, de forma opcional, una o varias celdas de aplicación de vCD.
 - Si desconectó las celdas del entorno existente, puede usar las direcciones IP originales para las celdas nuevas.
 - Si exportó una nueva ruta de acceso en el servidor NFS existente, puede utilizar este nuevo punto de montaje compartido para el nuevo entorno.

Consulte [Capítulo 6 Implementar el dispositivo de vCloud Director](#).

- 10 En cada celda recién implementada, ejecute el comando para detener el servicio de vCloud Director.

```
service vmware-vcd stop
```

- 11 Copie el archivo de volcado de la carpeta /tmp de la base de datos PostgreSQL externa en la carpeta /tmp de la celda principal del nuevo entorno.

Consulte el paso 5.

- 12 Cambie los permisos en el archivo de volcado.

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

- 13 Inicie sesión como **usuario raíz** en la consola de la celda principal recién implementada y transfiera la base de datos de vCloud Director de la base de datos externa a la base de datos integrada.

- a Cambie el usuario a postgres, conéctese al terminal de base de datos de psql y ejecute la instrucción para quitar la base de datos de vcloud.

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

- b Si el propietario de la base de datos externa existente no es vcloud, cree un usuario con el nombre que anotó en el paso 6.

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

- c Ejecute el comando pg_restore.

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

- d Si el nombre de la base de datos externa existente no es vcloud, cambie el nombre de la base de datos a vcloud utilizando el nombre que anotó en el paso 6.

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

- e Si el propietario de la base de datos del entorno de vCloud Director existente no es vcloud, cambie el propietario de la base de datos a vcloud y reasigne las tablas a 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 En cada celda recién implementada, realice una copia de seguridad de los datos de configuración y reemplácelos; a continuación, vuelva a configurar e iniciar el servicio de vCloud Director.

- a Realice una copia de seguridad de las propiedades y los archivos de certificado, y copie y reemplace estos archivos a partir de la ubicación en la base de datos de PostgreSQL externa del origen de migración en la que copió los archivos en el paso 7a.

Los archivos `global.properties`, `responses.properties`, `certificates` y `proxycertificates` están en `/opt/vmware/vcloud-director/etc/`.

Importante Si va a migrar a la versión 9.7.0.1 de vCloud Director o una versión posterior, también debe copiar y reemplazar el archivo `truststore` del origen de migración, así como realizar una copia de seguridad de este archivo, junto con el resto de los archivos.

- b Realice una copia de seguridad del archivo de almacén de claves que se encuentra en `/opt/vmware/vcloud-director/certificates.ks`.

No copie ni reemplace con el archivo de almacén de claves del origen de migración.

- c Ejecute el comando para volver a configurar el servicio de vCloud Director.

```
/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
```

Donde:

- El valor `--keystore-password` coincide con la contraseña **raíz** inicial del dispositivo.
- El valor `--database-password` coincide con la contraseña de la base de datos que configuró durante la implementación del dispositivo.
- El valor `--database-host` coincide con la dirección IP de red de `eth1` del dispositivo principal.
- El valor `--primary-ip` coincide con la dirección IP de red de `eth0` del dispositivo.
- El valor `--console-proxy-ip` coincide con la dirección IP de red de `eth0` del dispositivo.
- El valor `--console-proxy-port` coincide con el puerto del proxy 8443 de la consola del dispositivo.

Para obtener información sobre cómo solucionar problemas, consulte [Error al volver a configurar el servicio de vCloud Director cuando se realiza una migración al dispositivo de vCloud Director o una restauración en este](#).

- d Ejecute el comando para iniciar el servicio de vCloud Director.

```
service vmware-vcd start
```

Puede supervisar el progreso del inicio de la celda en `/opt/vmware/vcloud-director/logs/cell.log`.

- 15 Una vez que todas las celdas del nuevo grupo de servidores finalicen el proceso de inicio, compruebe que la migración del entorno de vCloud Director sea correcta.
 - a Abra la vCloud Director Web Console mediante la dirección IP de red de eth0 de cualquier celda del nuevo grupo de servidores, `https://eth0_IP_new_cell/cloud`.
 - b Inicie sesión en vCloud Director Web Console con las credenciales del **administrador del sistema** existentes.
 - c Compruebe que los recursos de vSphere y de nube estén disponibles en el nuevo entorno.
- 16 Después de la comprobación correcta de la migración de vCloud Director, utilice la vCloud Director Web Console para eliminar las celdas desconectadas que pertenezcan al entorno anterior de vCloud Director.
 - a En la pestaña **Administrar y supervisar**, haga clic en **Celdas de nube**.
 - b Haga clic con el botón secundario en el nombre de una celda y seleccione **Eliminar**.

Puede implementar el dispositivo de vCloud Director para agregar miembros al grupo de servidores del entorno migrado.

Qué hacer a continuación

El nuevo entorno del dispositivo de vCloud Director migrado utiliza certificados autofirmados. Para usar los certificados firmados correctamente del entorno anterior, en cada celda del nuevo entorno, siga estos pasos:

- 1 Copie y reemplace el archivo de almacén de claves de la celda anterior en `/opt/vmware/vcloud-director/data/transfer/certificates.ks`.
- 2 Ejecute el comando de la herramienta de administración de celdas para reemplazar los certificados.

Asegúrese de que `vcloud.vcloud` sea el propietario de este archivo.

```
/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 Reinicie el servicio de vCloud Director.

```
service vmware-vcd restart
```

Si agrega nuevos miembros a este grupo de servidores, las nuevas celdas del dispositivo se implementarán con estos certificados firmados correctamente.

Después de actualizar o migrar vCloud Director

13

Después de actualizar o migrar todos los servidores de vCloud Director y la base de datos compartida, puede actualizar las instancias de NSX Manager que ofrecen servicios de red a la nube. Después de eso, puede actualizar los hosts ESXi y las instancias de vCenter Server registradas en la instalación de vCloud Director.

Importante A partir de la versión 9.7, vCloud Director solo admite puertas de enlace Edge avanzadas. Debe convertir todas las puertas de enlace Edge no avanzadas heredadas en puertas de enlace avanzadas. Consulte <https://kb.vmware.com/kb/66767>.

Este capítulo incluye los siguientes temas:

- [Actualizar cada instancia de NSX Manager que esté asociada con un sistema vCenter Server adjunto](#)
- [Actualizar sistemas vCenter Server, hosts ESXi e instancias de NSX Edge](#)
- [Nuevos derechos en esta versión](#)

Actualizar cada instancia de NSX Manager que esté asociada con un sistema vCenter Server adjunto

Antes de actualizar un vCenter Server y los hosts ESXi registrados en vCloud Director, debe actualizar cada instancia de NSX Manager asociada a ese vCenter Server.

Al actualizar NSX Manager, se interrumpe el acceso a las funciones administrativas de NSX, aunque esto no afecta a los servicios de red. Puede actualizar NSX Manager antes o después de actualizar vCloud Director, sin importar que haya celdas de vCloud Directoren ejecución.

Para obtener información sobre la actualización de NSX, consulte la documentación de NSX para vSphere en <https://docs.vmware.com>.

Procedimiento

- 1 Actualice la instancia de NSX Manager asociada a cada vCenter Server registrado en su instalación de vCloud Director.
- 2 Después de haber actualizado todas las instancias de NSX Manager, puede actualizar los hosts ESXi y los sistemas vCenter Server registrados.

Actualizar sistemas vCenter Server, hosts ESXi e instancias de NSX Edge

Después de actualizar vCloud Director y NSX Manager, debe actualizar los sistemas vCenter Server y los hosts ESXi que estén registrados en vCloud Director. Después de actualizar todos los sistemas vCenter Server y los hosts ESXi conectados, puede actualizar las instancias de NSX Edge.

Requisitos previos

Verifique que ya haya actualizado cada instancia de NSX Manager asociada a los sistemas vCenter Server adjuntos a su nube. Consulte [Actualizar cada instancia de NSX Manager que esté asociada con un sistema vCenter Server adjunto](#).

Procedimiento

- 1 Deshabilite la instancia de vCenter Server.
 - a En la consola web de vCloud Director, haga clic en la pestaña **Gestionar y Supervisar** y, en el panel izquierdo, haga clic en **vCenters**.
 - b Haga clic con el botón secundario en el nombre de vCenter Server de destino y haga clic en **Deshabilitar**.
 - c Haga clic en **Sí**.
- 2 Actualice el sistema vCenter Server.

Para obtener información, consulte *Actualización de vCenter Server*.
- 3 Verifique todas las URL públicas de vCloud Director y las cadenas de los certificados.
 - a En la consola web de vCloud Director, haga clic en la pestaña **Administración** y, en el panel izquierdo, haga clic en **Direcciones públicas**.
 - b Verifique todas las direcciones públicas.
- 4 Actualice el registro de vCenter Server con vCloud Director.
 - a En la consola web de vCloud Director, haga clic en la pestaña **Gestionar y Supervisar** y, en el panel izquierdo, haga clic en **vCenters**.
 - b Haga clic con el botón secundario en el nombre de vCenter Server de destino y haga clic en **Actualizar**.
 - c Haga clic en **Sí**.

5 Actualice cada host ESXi que sea compatible con el sistema vCenter Server actualizado.

Consulte *Actualización de VMware ESXi*.

Importante Para garantizar que tiene suficiente capacidad de host actualizado para dar soporte a las máquinas virtuales de su nube, actualice los hosts en lotes pequeños. Cuando realice este paso, las actualizaciones de los agentes de host se completarán a tiempo para permitir que las máquinas virtuales vuelvan a migrar al host actualizado.

- a Utilice el sistema vCenter Server para poner el host en modo de mantenimiento y permitir la migración de todas las máquinas virtuales de dicho host a otro host.
 - b Actualice el host.
 - c Use el sistema vCenter Server para volver a conectar el host.
 - d Utilice el sistema vCenter Server para finalizar el modo de mantenimiento del host.
- 6** (opcional) Actualice las instancias de NSX Edge administradas por la instancia de NSX Manager asociada al sistema vCenter Server actualizado.

Las instancias de NSX Edge actualizadas presentan mejoras de rendimiento e integración. Puede usar NSX Manager o vCloud Director para actualizar las instancias de NSX Edge.

- Para obtener información sobre el uso de NSX Manager para actualizar instancias de NSX Edge, consulte la documentación de NSX para vSphere en <https://docs.vmware.com>.
- Para usar vCloud Director a fin de actualizar instancias de NSX Edge, debe trabajar en el objeto de red de vCloud Director que admite Edge:
 - La actualización correspondiente de un dispositivo de una puerta de enlace Edge se produce de manera automática cuando se utiliza la consola web de vCloud Director o vCloud API para restablecer una red que emplea la puerta de enlace Edge.
 - Al volver a implementar una puerta de enlace Edge, se actualiza el dispositivo de NSX Edge asociado.
 - Al restablecer una red de vApp en el contexto de la vApp, se actualiza el dispositivo de NSX Edge asociado a esa red. Si desea usar la consola web de vCloud Director para restablecer una red de vApp desde el interior del contexto de una vApp, desplácese hasta la pestaña **Redes** de la vApp, muestre sus detalles de red, haga clic con el botón secundario del ratón en la red de vApp y seleccione **Restablecer red**.

Para obtener más información sobre cómo volver a implementar puertas de enlace Edge y restablecer redes de vApp, consulte la ayuda en pantalla de la consola web de vCloud Director o la *Guía de programación de la API de vCloud*.

Pasos siguientes

Repita este procedimiento con los demás sistemas vCenter Server registrados en su instalación de vCloud Director.

Nuevos derechos en esta versión

vCloud Director 9.7 introduce nuevos derechos, que se recomienda agregar a cualquier función global existente publicada en los tenants.

Derecho	Descripción	Función predeterminada
SDDC: Ver SDDC	Permite ver todos los SDDC publicados en la organización. El administrador del sistema puede ver todos los SDDC.	Administrador del sistema y Administrador de organización
SDDC: Administrar SDDC	Permite agregar, quitar y editar SDDC.	Administrador del sistema
SDDC: Administrar proxy de SDDC	Permite agregar, quitar, habilitar y deshabilitar servidores proxy de SDDC.	Administrador del sistema
Aplicaciones de servicio: Ver aplicaciones de servicio	Permite ver la lista de aplicaciones de servicio registradas. Se utiliza para las cuentas VMC.	Administrador del sistema
Aplicaciones de servicio: Registrar SDDC de VMC	Permite crear, ver, editar y eliminar aplicaciones de servicio. Se utiliza para las cuentas VMC.	Administrador del sistema
Aplicaciones de servicio: Administrar aplicaciones de servicio	Permite registrar aplicaciones de servicio. Se utiliza para las cuentas VMC.	Administrador del sistema
Clúster de Edge: Ver clúster de Edge	Permite ver una lista de clústeres de Edge y recuperar un clúster de Edge individual.	Administrador del sistema y Administrador de organización
Clúster de Edge: Administrar clúster de Edge	Permite crear, editar y eliminar clústeres de Edge.	Administrador del sistema y Administrador de organización
vApp: Editar política de recursos informáticos de la máquina virtual	Permite que los usuarios cambien la política de recursos informáticos de una máquina virtual.	Administrador del sistema, Administrador de organización, Autor de catálogo y Autor de vApp
Puerta de enlace: Importar puerta de enlace Edge	Permite importar un enrutador de nivel 1 como una puerta de enlace Edge.	Administrador del sistema y Administrador de organización

Para obtener información sobre la administración de derechos y funciones, consulte la *Guía del portal para administradores de proveedores de servicios de vCloud Director*.

Solucionar problemas del dispositivo de vCloud Director

14

Si se produce un error en la implementación del dispositivo de vCloud Director o si el dispositivo no funciona correctamente, puede examinar los archivos de log del dispositivo para determinar la causa del problema.

El soporte técnico de VMware solicita de forma periódica información de diagnóstico sobre la gestión de las solicitudes de soporte. Puede utilizar el script `vmware-vcd-support` para recopilar información de registro de hosts y registros de vCloud Director. Para obtener más información sobre cómo recopilar información de diagnóstico para vCloud Director, consulte <https://kb.vmware.com/s/article/1026312>. Al ejecutar el script `vmware-vcd-support`, es posible que los registros incluyan información sobre las celdas con el estado `Con errores` que se dieron de baja o se reemplazaron. Consulte <https://kb.vmware.com/s/article/71349>.

Este capítulo incluye los siguientes temas:

- [Examinar los archivos de log en el dispositivo de vCloud Director](#)
- [La celda de vCloud Director no se puede iniciar después de la implementación del dispositivo](#)
- [Error al volver a configurar el servicio de vCloud Director cuando se realiza una migración al dispositivo de vCloud Director o una restauración en este](#)
- [Usar los archivos de registro para solucionar problemas de actualizaciones y revisiones de vCloud Director](#)
- [Error al buscar actualizaciones de vCloud Director](#)
- [Error al instalar la última actualización de vCloud Director](#)

Examinar los archivos de log en el dispositivo de vCloud Director

Después de implementar el dispositivo de vCloud Director, es posible examinar los logs de la base de datos y de primer arranque para detectar errores y advertencias.

Procedimiento

- 1 Inicie sesión directamente o utilice SSH en la consola del dispositivo de vCloud Director como **usuario raíz**.
- 2 Desplácese hasta `/opt/vmware/var/log`.

3 Examine los archivos de log.

- El archivo `firstboot` contiene información de registro relacionada con el primer arranque del dispositivo.
- El directorio `/opt/vmware/var/log/vcd/` contiene logs relacionados con la configuración del conjunto de herramientas de Replication Manager (repmgr), y la reconfiguración y la sincronización del dispositivo.
- El directorio `/opt/vmware/var/log/vcd/pg/` contiene logs relacionados con la copia de seguridad de la base de datos del dispositivo integrada.
- El archivo `/opt/vmware/etc/vami/ovfEnv.xml` contiene los parámetros de OVF de la implementación.

La celda de vCloud Director no se puede iniciar después de la implementación del dispositivo

El dispositivo de vCloud Director se implementó correctamente, pero puede que los servicios de vCloud Director no se inicien.

Problema

El servicio `vmware-vcd` está inactivo después de la implementación del dispositivo.

Causa

Si implementó una celda principal, es posible que los servicios de vCloud Director no se inicien debido a un almacenamiento del servicio de transferencia compartido de NFS que se rellena de antemano. Antes de implementar el dispositivo principal, el almacenamiento del servicio de transferencia compartido no debe contener un archivo `responses.properties` ni un directorio `appliance-nodes`.

Si implementó una celda de aplicación de vCD o en espera, es posible que los servicios de vCloud Director no se inicien debido a que falta el archivo `responses.properties` en el almacenamiento de transferencia compartido de NFS. Antes de implementar un dispositivo de aplicación de vCD o en espera, el almacenamiento del servicio de transferencia compartido debe contener el archivo `responses.properties`.

Solución

- 1 Inicie sesión directamente o utilice SSH en la consola del dispositivo de vCloud Director como **usuario raíz**.
- 2 Examine `/opt/vmware/var/log/vcd/setupvcd.log` en busca de mensajes de error relacionados con el almacenamiento de NFS.
- 3 Prepare el almacenamiento de NFS para el tipo de dispositivo.
- 4 Vuelva a implementar la celda.

Error al volver a configurar el servicio de vCloud Director cuando se realiza una migración al dispositivo de vCloud Director o una restauración en este

Cuando se realiza la migración o la restauración al dispositivo de vCloud Director, se puede producir un error al ejecutar el comando `configure`.

Problema

Durante el procedimiento para migrar o restaurar vCloud Director a un nuevo entorno de dispositivo de vCloud Director, debe ejecutar el comando `configure` para volver a configurar el servicio de vCloud Director en cada nueva celda. El comando `configure` puede generar un error con el mensaje de error `sun.security.validator.ValidatorException: error en la validación de la ruta PKIX: java.security.cert.CertPathValidatorException: error al comprobar la firma`.

Solución

- 1 En la celda de destino, ejecute el comando.

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

- 2 Espere 1 minuto y vuelva a ejecutar el comando `configure`.

Usar los archivos de registro para solucionar problemas de actualizaciones y revisiones de vCloud Director

Los archivos de registro se pueden examinar en busca de errores y advertencias cuando se aplican revisiones en el dispositivo de vCloud Director.

Problema

Si el comando `vamicli` devuelve un error, puede utilizar los archivos de registro para solucionar los problemas.

Solución

- 1 Inicie sesión directamente o utilice SSH en la consola del dispositivo de vCloud Director como **usuario raíz**.
- 2 Desplácese hasta el archivo de registro apropiado.
 - Si se produce un error en `vamicli update --check`, desplácese hasta `/opt/vmware/var/log/vami/vami.log`.
 - Si se produce un error en `vamicli update --install latest`, desplácese hasta `/opt/vmware/var/log/vami/updatecli.log`.
- 3 Examine el archivo de registro.

Error al buscar actualizaciones de vCloud Director

Cuando se buscan actualizaciones para el dispositivo de vCloud Director, se puede producir un error al ejecutar el comando `vamcli update --check`.

Problema

Durante el procedimiento de aplicación de una revisión en el dispositivo de vCloud Director, se ejecuta el comando `vamcli update --check` para buscar actualizaciones disponibles. El comando `vamcli update --check` puede generar el error `Error: Error al descargar el manifiesto`. Póngase en contacto con su proveedor.

Causa

La ruta de acceso al directorio del repositorio de actualizaciones no es correcta.

Solución

- 1 Ejecute el comando `vamcli` con la ruta de acceso correcta.

```
vamcli update --repo file:/root/local-update-repo
```

- 2 Vuelva a ejecutar el comando para buscar actualizaciones.

```
vamcli update --check
```

Error al instalar la última actualización de vCloud Director

Cuando instala las últimas actualizaciones en el dispositivo de vCloud Director, se puede producir un error al ejecutar el comando `vamcli update --install latest`.

Problema

Durante el procedimiento de aplicación de una revisión al dispositivo de vCloud Director, se ejecuta el comando `vamcli update --install latest` para aplicar la última revisión disponible. El comando `vamcli update --install latest` podría generar el error `Error: Error al ejecutar la instalación del paquete`.

Causa

El error se produce cuando no se puede acceder al servidor NFS.

Solución

- 1 Compruebe que se pueda acceder al servidor NFS montado en `/opt/vmware/vcloud-director/data/transfer`.
- 2 Vuelva a ejecutar el comando para aplicar la revisión disponible.

```
vamcli update --install latest
```

Desinstalación del software de vCloud Director

15

Use el comando `rpm` de Linux para desinstalar el software de vCloud Director de un servidor individual.

Procedimiento

- 1 Inicie sesión en el servidor de destino como **raíz**.
- 2 Desmonte el almacenamiento del servicio de transferencia que habitualmente se monta en `/opt/vmware/vcloud-director/data/transfer`.
- 3 Abra una ventana de consola, shell o terminal, y ejecute el comando de Linux `rpm`.

```
rpm -e vmware-phonehome vmware-vcloud-director vmware-vcloud-director-rhel
```

Si hay otros paquetes instalados que dependen del paquete `vmware-vcloud-director`, el sistema le pedirá que los desinstale antes de desinstalar vCloud Director.