

# Guía de instalación, configuración y actualización de vCloud Director

19 de septiembre de 2019  
VMware Cloud Director 10.0

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](http://www.vmware.com)

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

## **1** Descripción general de la instalación, configuración y actualización de vCloud Director 8

Arquitectura de vCloud Director 8

Planificación de la configuración 10

## **2** Requisitos de hardware y de software de vCloud Director 11

Requisitos de configuración de red para vCloud Director 12

Requisitos de seguridad de red 14

## **3** Antes de instalar vCloud Director o implementar el dispositivo de vCloud Director 16

Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux 16

Preparar el almacenamiento del servidor de transferencia 18

Instalar y configurar un broker AMQP de RabbitMQ 21

Descarga e instalación de la clave pública de VMware 22

Instalar y configurar NSX Data Center for vSphere para vCloud Director 23

Instalar y configurar NSX-T Data Center para vCloud Director 24

## **4** Creación y administración de certificados SSL para vCloud Director en Linux 26

Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux 26

Crear certificados SSL autofirmados para vCloud Director en Linux 27

Crear un almacén de claves de certificados SSL firmados por una entidad de certificación para vCloud Director en Linux 28

Crear un almacén de claves de certificados SSL firmados por una entidad de certificación con claves privadas importadas para vCloud Director en Linux 32

## **5** Instalar vCloud Director en Linux 34

Instalar vCloud Director en el primer miembro de un grupo de servidores 35

Configuración de conexiones de red y de base de datos 37

Referencia de configuración interactiva 39

Referencia de configuración sin supervisión 40

Proteger y reutilizar el archivo de respuesta 44

Instalar vCloud Director en un miembro adicional de un grupo de servidores 45

## **6** Implementar el dispositivo de vCloud Director 48

Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos 50

- Requisitos previos para implementar el dispositivo de vCloud Director 53
- Implementar el dispositivo de vCloud Director mediante vSphere Client 54
  - Directrices de tamaño del dispositivo de vCloud Director 55
  - Iniciar la implementación del dispositivo de vCloud Director 60
  - Personalizar el dispositivo de vCloud Director y finalizar la implementación 62
- Implementar el dispositivo de vCloud Director mediante VMware OVF Tool 64

## 7 Creación y administración de certificados SSL del dispositivo vCloud Director 72

- Implementar el dispositivo de vCloud Director con certificados comodín firmados para las comunicaciones de proxy de consola y HTTPS 72
- Crear e importar certificados SSL firmados por una entidad de certificación para el dispositivo de vCloud Director 74
- Importar claves privadas y certificados SSL firmados por una entidad de certificación en el dispositivo de vCloud Director 78
- Reemplazar un certificado autofirmado de interfaz de usuario de administración de dispositivos de vCloud Director y de una instancia integrada de PostgreSQL 80
- Renovar los certificados del dispositivo de vCloud Director 81

## 8 Configuración del dispositivo de vCloud Director 83

- Ver el estado de las celdas en un clúster de alta disponibilidad de la base de datos 84
- Recuperarse de un error de base de datos principal en un clúster de alta disponibilidad 84
- Recuperarse de un error de celda en espera en un clúster de alta disponibilidad 85
- Copia de seguridad y restauración de la base de datos integrada del dispositivo de vCloud Director 86
  - Realizar una copia de seguridad de la base de datos integrada del dispositivo de vCloud Director 86
  - Restaurar un entorno de dispositivo de vCloud Director con una configuración de base de datos de alta disponibilidad 87
- Configurar el acceso externo a la base de datos de vCloud Director 90
- Habilitar o deshabilitar el acceso SSH al dispositivo de vCloud Director 91
- Editar la configuración de DNS del dispositivo de vCloud Director 92
- Editar las rutas estáticas de las interfaces de red del dispositivo de vCloud Director 92
- Scripts de configuración en el dispositivo de vCloud Director 94
- Aumentar la capacidad de la base de datos de PostgreSQL integrada en un dispositivo de vCloud Director 94
- Modificar las configuraciones de PostgreSQL en el dispositivo de vCloud Director 96

## 9 Usar Replication Manager Tool Suite en la configuración de un clúster de alta disponibilidad 98

- Comprobar el estado de conectividad de un clúster de alta disponibilidad de la base de datos 99
- Comprobar el estado de replicación de un nodo en un clúster de alta disponibilidad de la base de datos 100
- Comprobar el estado de un clúster de alta disponibilidad de la base de datos 101

- Detectar un nodo principal anterior que vuelve a conectarse en un clúster de alta disponibilidad 102
- Cambiar las funciones de la celda principal y una celda en espera en un clúster de alta disponibilidad de la base de datos 104
- Eliminar del registro un nodo en espera con errores o inaccesible en un clúster de alta disponibilidad de la base de datos 106
- Eliminar del registro una celda principal con errores en un clúster de alta disponibilidad de la base de datos 106
- Eliminar del registro una celda en espera en ejecución en un clúster de alta disponibilidad de la base de datos 107

## **10 Referencia de la herramienta de administración de celdas 109**

- Configurar una instalación de vCloud Director 113
- Habilitar vCloud Director Web Console 115
- Deshabilitar el acceso de proveedores de servicios al endpoint de API heredado 117
- Administrar una celda 118
- Administrar aplicaciones de las celdas 119
- Actualización de las propiedades de conexión de la base de datos 121
- Detectar y reparar datos dañados del programador 124
- Generar certificados autofirmados para los endpoints de proxy de consola y HTTP 125
- Sustituir certificados para los endpoints de proxy de consola y HTTP 127
- Importar certificados SSL desde servicios externos 129
- Administrar la lista de cifrados SSL permitidos 130
- Administrar la lista de protocolos SSL permitidos 132
- Configurar recopilación de métricas 134
- Configurar una base de datos de métricas de Cassandra 137
- Recuperación de la contraseña del administrador del sistema 138
- Actualizar el estado de error de una tarea 139
- Configurar la administración de mensajes de auditoría 140
- Configurar plantillas de correo electrónico 142
- Encontrar máquinas virtuales huérfanas 143
- Unirse o abandonar el Programa de mejora de la experiencia del cliente de VMware 145
- Actualizar las opciones de configuración de la aplicación 146
- Configurar la limitación de sincronización del catálogo 147
- Solucionar errores de acceso a la interfaz de usuario de vCloud Director 149
- Depurar la detección de máquinas virtuales de vCenter 150
- Volver a generar direcciones MAC para redes extendidas multisitio 151
- Actualizar las direcciones IP de la base de datos en celdas de vCloud Director 154

## **11 Después de instalar vCloud Director o implementar el dispositivo de vCloud Director 156**

- Instalar archivos de Microsoft Sysprep en los servidores 156
- Cambiar la zona horaria del dispositivo de vCloud Director 157

[Personalizar direcciones públicas](#) 158

[Instalar y configurar una base de datos de Cassandra para almacenar datos de métricas históricas](#) 160

[Realizar configuraciones adicionales en la base de datos externa de PostgreSQL](#) 161

## **12 Actualización de vCloud Director** 163

[Actualizar el dispositivo de vCloud Director](#) 167

[Revertir un dispositivo de vCloud Director a la versión anterior cuando se produce un error en una actualización](#) 169

[Actualizar el dispositivo de vCloud Director mediante el repositorio de actualizaciones de VMware](#) 171

[Realizar una actualización orquestada de una instalación de vCloud Director](#) 172

[Actualizar manualmente una instalación de vCloud Director](#) 175

[Actualizar una celda de vCloud Director](#) 177

[Actualización de la base de datos de vCloud Director](#) 179

[Referencia de la utilidad de actualización de bases de datos](#) 180

## **13 Migrar al dispositivo de vCloud Director** 184

[Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director](#) 184

## **14 Después de actualizar o migrar vCloud Director** 190

[Actualizar cada instancia de NSX Manager que esté asociada con un sistema vCenter Server adjunto](#) 190

[Actualizar sistemas vCenter Server, hosts ESXi e instancias de NSX Edge](#) 191

## **15 Visualizar los registros de vCloud Director** 193

## **16 Solucionar problemas del dispositivo de vCloud Director** 195

[Examinar los archivos de log en el dispositivo de vCloud Director](#) 195

[La celda de vCloud Director no se puede iniciar después de la implementación del dispositivo](#) 196

[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](#) 197

[Usar los archivos de registro para solucionar problemas de actualizaciones y revisiones de vCloud Director](#) 197

[Error al buscar actualizaciones de vCloud Director](#) 198

[Error al instalar la última actualización de vCloud Director](#) 198

## **17 Desinstalación del software de vCloud Director** 199

# 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<sup>®</sup> for Service Providers, así como la configuración para que este software funcione con VMware vSphere<sup>®</sup>, VMware NSX<sup>®</sup> for vSphere<sup>®</sup> y VMware NSX-T<sup>™</sup> 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.

# 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.

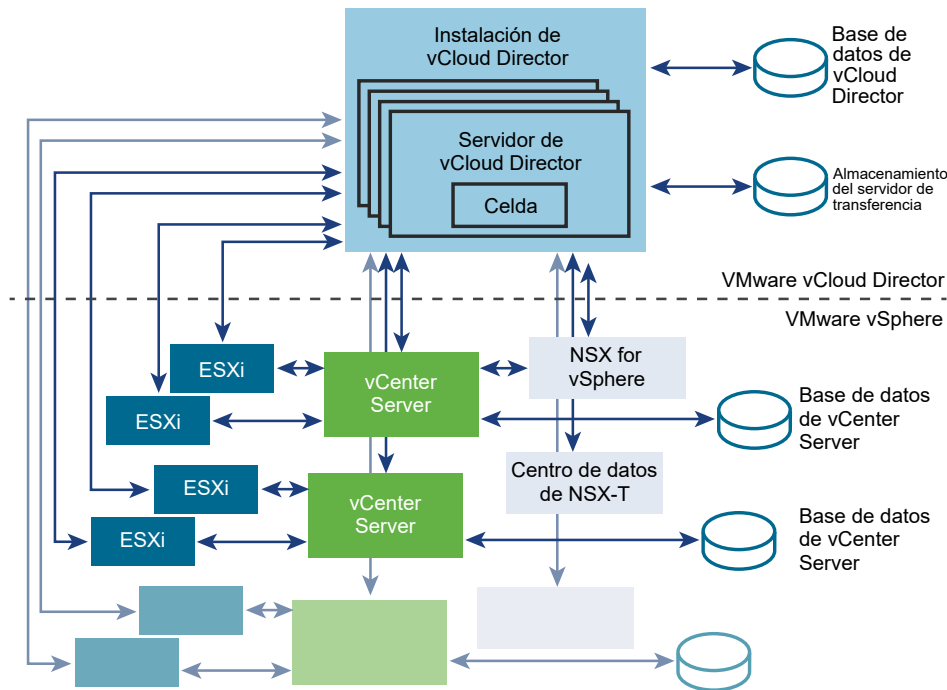
---



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 o NSX-T Manager.

Para obtener información sobre cómo agregar recursos de red y vSphere, consulte la *Guía del portal para administradores de proveedores de servicios 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 [Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux](#).

# 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](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 10.0* 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 10.0*.

## 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 Service Provider Admin Portal. 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.

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

Puerto	Protocolo	Comentarios
902	TCP	Conexiones de vCenter y de ESXi.
903	TCP	Conexiones de vCenter y de ESXi.
920	TCP, UDP	rpc.statd de NFS utilizado por el servicio de transferencia.
5432	TCP	Puerto predeterminado de base de datos de PostgreSQL
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:

- [Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux](#)
- [Preparar el almacenamiento del servidor de transferencia](#)
- [Instalar y configurar un broker AMQP de RabbitMQ](#)
- [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](#)

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

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 instancia de base de datos de PostgreSQL y crear la cuenta de usuario de base de datos de vCloud Director.

Las bases de datos de PostgreSQL tienen requisitos de configuración específicos cuando se utilizan con vCloud Director.

Debe crear un esquema de base de datos dedicado independiente para que lo utilice vCloud Director. vCloud Director no puede compartir un esquema de base de datos con ningún otro producto de VMware.



vCloud Director admite conexiones SSL a la 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](#).

---

**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

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

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 `vcld` se crea con el siguiente comando.

```
create user vcld;
```

#### 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 `vcld` como propietario de la base de datos.

```
create database vcld owner vcld;
```

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

El siguiente comando asigna la contraseña `vclooudpass` al propietario de la base de datos `vclooud`.

```
alter user vcloud password 'vclooudpass';
```

- 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 `vclooud`.

```
alter role vcloud 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](#).

## 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.

## Instalar y configurar un broker 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 el menú principal () de vCloud Director Service Provider Admin Portal, seleccione **Administración**.
- 2 En el panel izquierdo, en **Configuración**, haga clic en **Extensibilidad**.
- 3 Haga clic en **Extensibilidad** y, a continuación, en **Editar** en la sección **Broker AMQP**.
- 4 Active el botón de alternancia **Utilizar SSL**.
- 5 Active el botón de alternancia **Aceptar todos los certificados** o proporcione uno de los siguientes elementos:
  - Un nombre de ruta de certificado SSL
  - Un nombre de ruta y una contraseña de almacén de confianza de JCEKS

## 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](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 12 Actualización 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 desea que la instalación de vCloud Director utilice recursos de red de NSX-T Data Center, debe instalar y configurar NSX-T Data Center.

---

**Importante** Para configurar los objetos y las herramientas de NSX-T Data Center, utilice la interfaz de usuario de políticas simplificada y las API de políticas que corresponden a la interfaz de usuario simplificada. Para obtener más información, consulte la descripción general de NSX-T Manager en la *Guía de administración de NSX-T Data Center*.

---

Para obtener la información más reciente acerca de la compatibilidad entre vCloud Director y otros productos VMware, consulte las [matrices de interoperabilidad de productos VMware](#).

Para obtener más información sobre los requisitos de red, consulte [Requisitos de configuración de red para vCloud Director](#).

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 12 Actualización de vCloud Director](#).

### Requisitos previos

Familiarícese con NSX-T Data Center.

### Procedimiento

- 1 Implemente y configure los dispositivos virtuales de NSX-T Manager.

Si desea obtener más información sobre la implementación de NSX-T Manager, consulte la *Guía de instalación de NSX-T Data Center*.

- 2 Cree zonas de transporte en función de los requisitos de redes.

Para obtener más información sobre la creación de zonas de transporte, consulte la *Guía de instalación de NSX-T Data Center*.

---

### Nota

- 3 Implemente y configure nodos de Edge y un clúster de Edge.

Para obtener más información sobre la creación de NSX Edge, consulte la *Guía de instalación de NSX-T Data Center*.



**4** Configure los nodos de transporte del host ESXi.

Para obtener más información sobre cómo configurar un nodo de transporte de host administrado, consulte la *Guía de instalación de NSX-T Data Center*.

**5** Cree una puerta de enlace de nivel 0.

Para obtener más información sobre la creación de nivel 0, consulte la *Guía de administración de NSX-T Data Center*.

**Pasos siguientes**

Después de instalar vCloud Director, puede hacer lo siguiente:

**1** Registrar la instancia de NSX-T Manager en la nube.

Para obtener información sobre el registro de una instancia de NSX-T Manager, consulte la *Guía del portal para administradores de proveedores de servicios de vCloud Director*.

**2** Crear un grupo de redes respaldado por una zona de transporte de NSX-T Data Center.

Para obtener más información sobre la creación de un grupo de redes respaldado por una zona de transporte de NSX-T Data Center, consulte la *Guía del portal para administradores de proveedores de servicios de vCloud Director*.

**3** Importar la puerta de enlace de nivel 0 como una red externa.

Para obtener más información sobre la inclusión de una red externa que esté respaldada por un enrutador lógico de nivel 0 de NSX-T Data Center, consulte la *Guía del portal para administradores de proveedores de servicios de vCloud Director*.

# 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 HTTP](#).
- 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 la [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 la [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 12 Actualización 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 la [Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux](#). 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.

## Pasos siguientes

Use el comando `system-setup` de la herramienta de administración de celdas para inicializar la base de datos del grupo de servidores con una cuenta de administrador del sistema y la información relacionada. Consulte la [Configurar una instalación 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 archivo-de-instalación
```

- 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 [Capítulo 10 Referencia de la herramienta de administración de celdas](#).

### 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/configure options -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.  <b>Nota</b> 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 <a href="#">Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux</a> .
Contraseña de clave privada del certificado SSL de HTTP	Consulte <a href="#">Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux</a> .
Contraseña de clave privada del certificado de SSL de proxy de la consola	Consulte <a href="#">Consideraciones previas a la creación de certificados SSL para vCloud Director en Linux</a> .

**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"> <li>■ Para omitir, presione Intro.</li> <li>■ Para habilitar, introduzca la dirección IP o el nombre del host de syslog.</li> </ul>
Si se habilitó el registro de auditoría remoto, el puerto UDP del host de syslog	El valor predeterminado es 514.
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	El valor predeterminado es 5432.
Nombre de la base de datos	El valor predeterminado es vcloud.
Nombre de usuario de la base de datos	Consulte la <a href="#">Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux</a> .
Contraseña de la base de datos	Consulte la <a href="#">Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux</a> .
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 <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a>, 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 <a href="#">Capítulo 10 Referencia de la herramienta de administración de celdas</a>.</p> <p>Para unirse al programa, introduzca <b>y</b>.</p> <p>Si prefiere no unirse al programa CEIP de VMware, introduzca <b>n</b>.</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>	Puede configurar la base de datos de PostgreSQL para que requiera una conexión SSL bien firmada desde vCloud Director. Si desea configurar la base de datos de PostgreSQL para que use un certificado autofirmado o privado, consulte <a href="#">Realizar configuraciones adicionales en la base de datos externa de PostgreSQL</a> .
<code>--database-host (-dbhost)</code>	Dirección IP o nombre de dominio completo del host de base de datos de vCloud Director	Consulte la <a href="#">Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux</a> .
<code>--database-name (-dbname)</code>	Nombre del servicio de base de datos	Consulte la <a href="#">Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux</a> .
<code>--database-password (-dbpassword)</code>	Contraseña para el usuario de la base de datos. Puede ser un valor nulo.	Consulte la <a href="#">Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux</a> .
<code>--database-port (-dbport)</code>	Número de puerto usado por el servicio de base de datos en el host de base de datos	Consulte la <a href="#">Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux</a> .

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

Opción	Argumento	Descripción
<code>--database-type (-dbtype)</code>	Tipo de la base de datos. El tipo admitido es postgres.	Opcional. El tipo de base de datos se establecerá en postgres de forma predeterminada. Consulte la <a href="#">Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux</a> .
<code>--database-user (-dbuser)</code>	Nombre de usuario del usuario de la base de datos	Consulte la <a href="#">Configurar una base de datos de PostgreSQL externa para vCloud Director en Linux</a> .
<code>--enable-ceip</code>	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 <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> , 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 <a href="#">Capítulo 10 Referencia de la herramienta de administración de celdas</a> .
<code>--uuid (-g)</code>	Ninguno	Genera un nuevo identificador único para la celda.
<code>--primary-ip (-ip)</code>	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> .
<code>--primary-port-http</code>	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
<code>--primary-port-https</code>	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

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

Opción	Argumento	Descripción
--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 sys log 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 sys log 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><b>Importante</b> 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 postgres -dbhost 10.150.10.78 -dbname postgresql-db-name -dbuser vcloud --enable-ceip true \
-dbpassword P055word -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 postgres -dbhost 10.150.10.78 -dbname postgresql-db-name \
-dbuser vcloud -dbpassword P055word -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 archivo-de-instalación
```

- 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 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.

- 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 mediante la herramienta de administración de celdas con el subcomando `system-setup`. Consulte la [Configurar una instalación 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) 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.

---

**Nota** Las redes eth0 y eth1 deben colocarse en subredes independientes.

---

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

Después de crear el dispositivo de vCloud Director, puede utilizar las funciones de redes de vSphere para agregar una nueva tarjeta de interfaz de red (NIC). Consulte la información [Agregar un adaptador de red a una máquina virtual](#) en la guía *Administrar máquinas virtuales de vSphere*.

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 Client](#)
- [Implementar el dispositivo de vCloud Director mediante VMware OVF Tool](#)

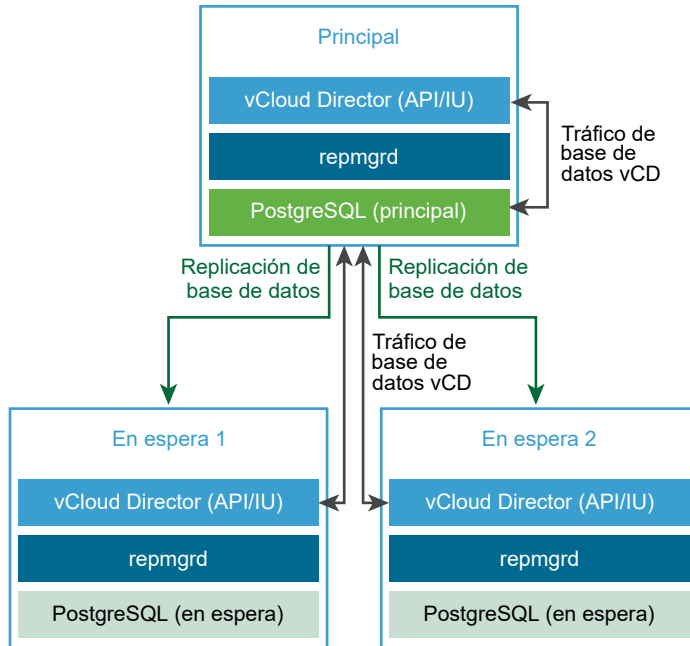
## Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos

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 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 vCloud Director Service Provider Admin Portal en `https://primary_eth0_ip_address/provider`.
- 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.

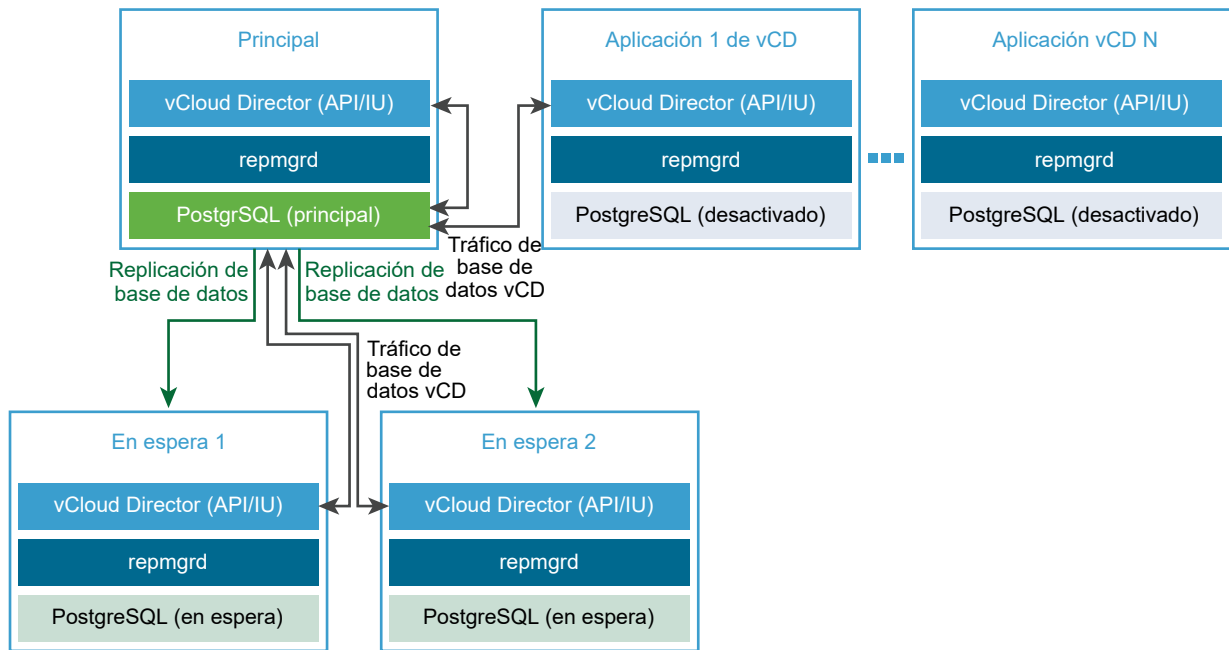
**Nota** Después de la implementación inicial del dispositivo en espera, Replication Manager comienza a sincronizar su base de datos con la base de datos del dispositivo principal. Durante este período, la base de datos de vCloud Director y, por tanto, la interfaz de usuario de vCloud Director no están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

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



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

**Nota** Puede implementar un clúster de vCloud Director con una celda principal y sin celdas en espera ni celdas de aplicación. VMware no admite implementaciones de una única celda en un entorno de producción, ya que se trata de un único origen de error desde una perspectiva de base de datos. Las implementaciones de una única celda no reciben soporte para problemas relacionados con el rendimiento o la estabilidad.

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 `vcloud` y el usuario de la base de datos es `vcloud`.

- 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 vCloud Director Service Provider Admin Portal en `https://dirección_ip_eth0_principal/proveedor`.
- 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 broker AMQP de RabbitMQ.](#)

## Métodos de implementación del dispositivo de vCloud Director

- [Implementar el dispositivo de vCloud Director mediante 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 Client

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

Al agregar dispositivos adicionales o de reemplazo a un clúster de base de datos, la vCPU y la RAM deben coincidir con las de las celdas principal y en espera existentes en el clúster.

La versión de OVA del modo en espera recién implementado debe ser la misma que la de los dispositivos existentes en el clúster. Para ver la versión de los dispositivos en ejecución, consulte la información de la sección Acerca de en la interfaz de usuario de administración de dispositivos. El dispositivo se distribuye con un nombre con el formato `VMware Cloud 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 Cloud Director-10.0.0.0-9229800_OVA10.ova`.

---

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 Directrices de tamaño del dispositivo de vCloud Director

Según sus necesidades, puede tener diferentes configuraciones del grupo de servidores basado en el dispositivo de vCloud Director y diferentes tamaños de las instancias de dispositivos virtuales de vCloud Director.

### 2 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).

### 3 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 direcciones públicas](#).
- Para agregar miembros al grupo de servidores de vCloud Director, repita el procedimiento.
- Para introducir la clave de licencia, inicie sesión en vCloud Director Service Provider Admin Portal.
- 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](#).

## Directrices de tamaño del dispositivo de vCloud Director

Según sus necesidades, puede tener diferentes configuraciones del grupo de servidores basado en el dispositivo de vCloud Director y diferentes tamaños de las instancias de dispositivos virtuales de vCloud Director.

## Descripción general

Para garantizar que el clúster pueda admitir una conmutación por error automatizada si se produce un error en una celda principal, la implementación mínima de vCloud Director debe constar de una celda principal y dos celdas en espera. El entorno permanece disponible en cualquier escenario de error en el que una de las celdas se desconecta por cualquier motivo. Si se produce un error en espera, hasta que se vuelva a implementar la celda con errores, el clúster opera en un estado totalmente funcional, con cierta degradación del rendimiento. Consulte la [Implementaciones de dispositivos y configuración de alta disponibilidad de bases de datos](#).

El dispositivo de vCloud Director tiene cuatro tamaños que puede seleccionar durante la implementación: pequeño, mediano, grande y extragrande (VVD). El tamaño de dispositivo pequeño es adecuado para la evaluación de laboratorio, y este documento no proporciona instrucciones sobre la configuración de dispositivos pequeños. La tabla de opciones de tamaño proporciona las especificaciones de las opciones restantes y los casos de uso más adecuados para un entorno de producción. La configuración extragrande coincide con el perfil de escala de [VMware Validated Designs \(VVD\) para proveedores de nube](#).

Para crear tamaños personalizados más grandes, los **administradores del sistema** pueden ajustar el tamaño de las celdas implementadas.

La configuración más pequeña recomendada para implementaciones de producción es una implementación de tres nodos de dispositivos virtuales de tamaño mediano.

---

**Nota** Puede implementar un clúster de vCloud Director con una celda principal y sin celdas en espera ni celdas de aplicación. VMware no admite implementaciones de una única celda en un entorno de producción, ya que se trata de un único origen de error desde una perspectiva de base de datos. Las implementaciones de una única celda no reciben soporte para problemas relacionados con el rendimiento o la estabilidad.

---

## Opciones de tamaño del dispositivo de vCloud Director

Puede utilizar la siguiente guía de decisión para calcular el tamaño del dispositivo para su entorno.

	Mediana	Grande	Extragrande (VVD)
Casos de uso recomendados	Entornos de producción pequeños o laboratorios	Entorno de producción	Producción con integraciones y supervisión de API
Implementación de vRealize Operations Management Pack en el entorno de vCloud Director	No	No	Sí
Habilitación de métricas de máquina virtual de Cassandra en vCloud Director	No	No	Sí
Número aproximado de usuarios o clientes simultáneos que acceden a la API durante un período máximo de 30 minutos.	< 50	< 100	< 100
Máquinas virtuales administradas	5000	5000	15000



## Definiciones de configuración

**Nota** vCloud Director 9.7 y los dispositivos posteriores `primary-large` y `standby-large`, de forma predeterminada, no tienen las 16 vCPU necesarias para una configuración de clúster de HA grande. Si desea tener una configuración de dispositivo de vCloud Director grande, después de la implementación, debe cambiar manualmente las vCPU de celda principal y en espera a 16.

	Mediana	Grande	Extragrande (VVD)
Configuración del clúster de HA	1 celda principal + 2 celdas en espera	1 celda principal + 2 celdas en espera + 1 celda de aplicación	1 celda principal + 2 celdas en espera + 2 celdas de aplicación
Celda principal o en espera de vCPU	8	16	24
Celda de aplicación de vCPU	N/D	8	8
Celda principal o en espera de RAM	16 GB	24 GB	32 GB
Celda de aplicación de RAM	N/D	8	8
Relación entre vCPU y núcleo físico	1:1	1:1	1:1
Personalización de PostgreSQL en celdas principales y en espera	shared_buffers = '3 GB'; effective_cache_size = '9 GB'; work_mem = '8 MB'; maintenance_work_mem = '1 GB'; max_worker_processes = '8';	shared_buffers = '5 GB'; effective_cache_size = '15 GB'; work_mem = '8 MB'; maintenance_work_mem = '1 GB'; max_worker_processes = '16';	shared_buffers = '7 GB'; effective_cache_size = '21 GB'; work_mem = '8 MB'; maintenance_work_mem = '1 GB'; max_worker_processes = '24';

### Cómo detectar si el sistema tiene un tamaño insuficiente

En una celda de vCloud Director, el uso de CPU o memoria crece y alcanza una meseta en un nivel alto, es decir, un nivel cerca de su capacidad. La celda de vCloud Director también podría perder la conexión con la base de datos.

### Cómo detectar si el número de celdas del sistema es insuficiente

En los archivos `vcloud-container-debug.log` y `cell-runtime.log` de cualquiera de las celdas de vCloud Director, verá entradas similares a `org.apache.tomcat.jdbc.pool.PoolExhaustedException: [pool-jetty-XXXXX] Timeout: Pool empty. Unable to fetch a connection in 20 seconds, none available`. La celda de vCloud Director también podría perder la conexión con la base de datos.

**Nota** Según la configuración de conexión de base de datos predeterminada, todas las configuraciones se limitan a un máximo de 6 celdas de tipo principal, en espera y de aplicación.

## Cómo personalizar el tamaño del dispositivo

Para ajustar el tamaño del dispositivo de vCloud Director con una de las configuraciones admitidas, después de ejecutar el implementador del dispositivo de vCloud Director, debe seguir este procedimiento en todas las celdas.

- 1 Compruebe que tiene el número necesario de celdas para la configuración seleccionada.
- 2 Ajuste la memoria y la vCPU de todas las celdas para que coincidan con una de las configuraciones admitidas que desee.

**Importante** La cantidad de RAM y vCPU debe ser la misma para todas las celdas principales y en espera.

- 3 Inicie sesión en el sistema operativo del dispositivo principal como **raíz** directamente o mediante un cliente SSH.
- 4 Cambie el usuario a **postgres**.

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

- 5 Para actualizar el archivo de configuración `postgresql.auto.conf`, ejecute los siguientes comandos.

Tipo de configuración	Descripción
Mediana	<pre>psql -c "ALTER SYSTEM set shared_buffers = '3GB';" psql -c "ALTER SYSTEM set effective_cache_size = '9GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '8';"</pre>
Grande	<pre>psql -c "ALTER SYSTEM set shared_buffers = '5GB';" psql -c "ALTER SYSTEM set effective_cache_size = '15GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '16';"</pre>
Extragrande	<pre>psql -c "ALTER SYSTEM set shared_buffers = '7GB';" psql -c "ALTER SYSTEM set effective_cache_size = '21GB';" psql -c "ALTER SYSTEM set work_mem = '8MB';" psql -c "ALTER SYSTEM set maintenance_work_mem = '1GB';" psql -c "ALTER SYSTEM set max_worker_processes= '24';"</pre>

6 Vuelva al usuario **raíz** mediante la ejecución del comando `exit`.

7 Reinicie el proceso de `vpostgres`.

```
systemctl restart vpostgres
```

8 Vuelva a cambiar el usuario a **postgres**.

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

9 Para cada nodo en espera, copie el archivo `postgresql.auto.conf` en el nodo y reinicie el proceso de `vpostgres`.

a Copie `postgresql.auto.conf` del nodo principal al nodo en espera.

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

b Reinicie el proceso de `vpostgres`.

```
systemctl restart vpostgres
```

Para ajustar el tamaño del dispositivo de vCloud Director con una configuración personalizada, después de ejecutar el implementador del dispositivo de vCloud Director, debe seguir este procedimiento en todas las celdas.

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

2 Para ver y tomar nota de la información de vCPU, ejecute el siguiente comando.

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

3 Para ver y tomar nota de la información de RAM, ejecute el siguiente comando.

La RAM que se indica a continuación se encuentra en KB y debe convertirla a GB dividiendo por 1.024.000.

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

4 Calcule el valor de `shared_buffers` para que sea un cuarto del total de RAM menos 4 GB.

$shared\_buffers = 0,25 * (total\ de\ RAM - 4\ GB)$

5 Calcule el valor de `effective_cache_size` para que sea tres cuartos del total de RAM menos 4 GB.

$effective\_cache\_size = 0,75 * (total\ de\ RAM - 4\ GB)$

6 Calcule el valor de `max_worker_processes` para que sea el número de vCPU.

7 Cambie el usuario a **postgres**.

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

- 8 Actualice el archivo de configuración `postgresql.auto.conf` ejecutando los siguientes comandos y sustituyendo con los valores calculados.

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

- 9 Vuelva al usuario **raíz** mediante la ejecución del comando `exit`.
- 10 Reinicie el proceso de `vpostgres`.

```
systemctl restart vpostgres
```

- 11 Vuelva a cambiar el usuario a **postgres**.

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

- 12 Para cada nodo en espera, copie el archivo `postgresql.auto.conf` en el nodo y reinicie el proceso de `vpostgres`.

- a Copie `postgresql.auto.conf` del nodo principal al nodo en espera.

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

- b Reinicie el proceso de `vpostgres`.

```
systemctl restart vpostgres
```

## 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
<b>Principal-pequeña</b>	<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>
<b>Principal-grande</b>	<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>
<b>En espera-pequeña</b>	<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>
<b>En espera-grande</b>	<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>
<b>Celda de aplicación de vCD</b>	<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.

---

**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
<b>Servidor NTP</b>	El nombre de host o la dirección IP del servidor NTP que se usará.
<b>Contraseña raíz inicial</b>	<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><b>Importante</b> 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><b>Nota</b> El asistente de implementación de OVF no valida la contraseña raíz inicial con los criterios de contraseña.</p>
<b>Caducar contraseña raíz después de primer inicio de sesión</b>	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.

Configuración	Descripción
Habilitar SSH	Opción deshabilitada de forma predeterminada.
Montaje de NFS para la ubicación del archivo de transferencia	Consulte <a href="#">Preparar el almacenamiento del servidor de transferencia</a> .

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

- Si desea implementar el primer miembro de un grupo de servidores, en la sección **Configurar VCD: necesario únicamente para dispositivos "principales"**, introduzca los detalles de la base de datos, cree la cuenta de **administrador del sistema** y configure el 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 <b>vcloud</b> .
Nombre del usuario administrador	El nombre de usuario para la cuenta de <b>administrador del sistema</b> . De forma predeterminada, es administrator.
Nombre completo del administrador	El nombre completo del <b>administrador del sistema</b> . De forma predeterminada, es vCD Admin.
Contraseña del usuario administrador	La contraseña para la cuenta de <b>administrador del sistema</b> .
Correo electrónico del administrador	La dirección de correo electrónico del <b>administrador del sistema</b> .
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.

- (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**.

Si desea acceder a los hosts a través de una ruta de puerta de enlace no predeterminada, es posible que necesite proporcionar rutas estáticas. 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 se encuentra en eth0. En la mayoría de los casos, esta opción puede permanecer vacía.

Las rutas estáticas deben formar una lista de especificaciones de ruta 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, 172.16.200.253**.

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

Configuración	Descripción
<b>Puerta de enlace predeterminada</b>	La dirección IP de la puerta de enlace predeterminada para el dispositivo.
<b>Nombre de dominio</b>	El dominio de búsqueda de DNS (por ejemplo, <i>mydomain.com</i> ).
<b>Ruta de búsqueda de dominios</b>	Una lista separada por comas o espacios de nombres de dominio para la búsqueda de nombres de host de dispositivo (por ejemplo, <i>subdomain.example.com</i> ).  <b>Nota</b> El nombre de dominio que ha introducido en el cuadro de texto Nombre de dominio es el primer elemento de la lista de rutas de acceso de búsqueda de dominios.
<b>Servidores de nombres de dominio</b>	La dirección IP del servidor de nombres de dominio para el dispositivo.
<b>Dirección IP de red de eth0</b>	La dirección IP de la interfaz eth0.
<b>Máscara de red de eth0</b>	El prefijo o la máscara de la interfaz eth0.
<b>Dirección IP de red de eth1</b>	La dirección IP de la interfaz eth1.
<b>Máscara de red de eth1</b>	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.
- [Cambiar la zona horaria del dispositivo de vCloud Director](#)

## 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*.

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

Al agregar dispositivos adicionales o de reemplazo a un clúster de base de datos, la vCPU y la RAM deben coincidir con las de las celdas principal y en espera existentes en el clúster.

La versión de OVA del modo en espera recién implementado debe ser la misma que la de los dispositivos existentes en el clúster. Para ver la versión de los dispositivos en ejecución, consulte la información de la sección Acerca de en la interfaz de usuario de administración de dispositivos. El dispositivo se distribuye con un nombre con el formato VMware Cloud Director-*v.v.v-  
nnnnnn\_OVF10.ova*, donde *v.v.v* representa la versión de producto y *nnnnnn*, el número de compilación. Por ejemplo: VMware Cloud Director-10.2.0.0-9229800\_OVA10.ova.

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 vSphere Client. Consulte la [Implementar el dispositivo de vCloud Director mediante vSphere Client](#).

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

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.

Opción	Valor	Descripción
<code>--net:"eth0 Network"</code>	<code>portgroup_on_vc_for_eth0</code>	La red de destino para la red eth0 del dispositivo.  <b>Importante</b> Debe ser diferente de la red de destino eth1.
<code>--net:"eth1 Network"</code>	<code>portgroup_on_vc_for_eth1</code>	La red de destino para la red eth1 del dispositivo.  <b>Importante</b> 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 <b>root</b> al dispositivo.
<code>--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"</code>	<code>true</code> o <code>false</code>	Determina si se debe continuar usando o no la contraseña inicial después del primer inicio de sesión.

Opción	Valor	Descripción
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director" <del>nfsexport</del>	<del>nfsexport</del> <i>nfs_mount_path</i>	La dirección IP y la ruta de exportación del servidor NFS externo. Solo se usa para una celda principal.
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director" <del>ntp-server</del>	<del>ntp-server</del> <i>ip_address</i>	La dirección IP del servidor de tiempo.
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director" <del>varoot-password</del>	<del>varoot-password</del> <i>password</i>	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.  <b>Importante</b> 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" <del>db_pwd</del>	<del>db_pwd</del> <i>password</i>	La contraseña de la base de datos del usuario <b>vcloud</b> . Solo se usa para una celda principal.
--prop:"vcloudwiz.admin_email.VMware_vCloud_Director" <del>admin_email</del>	<del>admin_email</del> <i>email_address</i>	La dirección de correo electrónico de la cuenta de <b>administrador del sistema</b> . Solo se usa para una celda principal.
--prop:"vcloudwiz.admin_fname.VMware_vCloud_Director" <del>admin_fname</del>	<del>admin_fname</del> <i>name</i>	El nombre para la cuenta de <b>administrador del sistema</b> . Solo se usa para una celda principal.
--prop:"vcloudwiz.admin_pwd.VMware_vCloud_Director" <del>admin_pwd</del>	<del>admin_pwd</del> <i>password</i>	La contraseña para la cuenta de <b>administrador del sistema</b> . Solo se usa para una celda principal.
--prop:"vcloudwiz.admin_uname.VMware_vCloud_Director" <del>admin_uname</del>	<del>admin_uname</del> <i>username</i>	El nombre de usuario para la cuenta de <b>administrador del sistema</b> . Solo se usa para una celda principal.
--prop:"vcloudwiz.inst_id.VMware_vCloud_Director" <del>inst_id</del>	<del>inst_id</del> <i>id</i>	El identificador de instalación de vCloud Director. Solo se usa para una celda principal.
--prop:"vcloudconf.sys_name.VMware_vCloud_Director" <del>sys_name</del>	<del>sys_name</del> <i>name</i>	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</code>	<code>Directional cidr, ip_address1 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, <b>172.16.100.253 172.16.100/19, 172.16.200.253.</b>
<code>--prop:"vcloudnet.routes1.VMware_vCloud_Director</code>	<code>Directional cidr, ip_address1 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, <b>172.16.100.253 172.16.100/19, 172.16.200.253.</b>

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"> <li>■ 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.</li> <li>■ 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.</li> <li>■ 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.</li> <li>■ 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</li> </ul>

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"> <li>■ 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.</li> </ul> <p><b>Importante</b> 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

**Importante** Antes de ejecutar el comando VMware OVF Tool, reemplace las contraseñas de `vcloudapp.varoot-passwordVMware_vCloud_Director`, `vcloudconf.db_pwdVMware_vCloud_Director` y `vcloudconf.admin_pwd.VMware_vCloud_Director` por sus propias contraseñas seguras.

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MyAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.142" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.24" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
```

```
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.db_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_email.VMware_vCloud_Director"="admin@mycompany.com" \
--prop:"vcloudconf.admin_fname.VMware_vCloud_Director"="vcdadmin" \
--prop:"vcloudconf.admin_pwd.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.admin_uname.VMware_vCloud_Director"="administrator" \
--prop:"vcloudconf.inst_id.VMware_vCloud_Director"="59" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MyAppliance" \
--deploymentOption="primary-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_datacenter_name/host/vc_cluster_name
```

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

**Importante** Antes de ejecutar el comando VMware OVF Tool, reemplace la contraseña de vcloudapp.varoot-password.VMware\_vCloud\_Director por su propia contraseña segura.

```
ovftool \
--noSSLVerify \
--acceptAllEulas \
--datastore='datastore6' \
--allowAllExtraConfig \
--net:"eth0 Network"="My_UI_API_Network" \
--net:"eth1 Network"="My_Internal_DB_Services_Network" \
--name=MySecondAppliance \
--diskMode=thin \
--prop:"vami.ip0.VMware_vCloud_Director"="10.0.0.143" \
--prop:"vami.ip1.VMware_vCloud_Director"="172.18.41.25" \
--prop:"vami.DNS.VMware_vCloud_Director"="10.0.0.2" \
--prop:"vami.domain.VMware_vCloud_Director"="mycompany.com" \
--prop:"vami.gateway.VMware_vCloud_Director"="10.0.0.1" \
--prop:"vami.netmask0.VMware_vCloud_Director"="255.255.0.0" \
--prop:"vami.netmask1.VMware_vCloud_Director"="255.255.224.0" \
--prop:"vami.searchpath.VMware_vCloud_Director"="eng.mycompany.com" \
--prop:"vcloudapp.enable_ssh.VMware_vCloud_Director"="False" \
--prop:"vcloudapp.expire_root_password.VMware_vCloud_Director"="True" \
--prop:"vcloudapp.nfs_mount.VMware_vCloud_Director"="10.0.0.96:/data/transfer" \
--prop:"vcloudapp.ntp-server.VMware_vCloud_Director"="time.mycompany.com" \
--prop:"vcloudapp.varoot-password.VMware_vCloud_Director"="place-secure-password-here" \
--prop:"vcloudconf.sys_name.VMware_vCloud_Director"="MySecondAppliance" \
--deploymentOption="standby-small" \
--powerOn "/MyPath/VMware_vCloud_Director-version_number_OVF10.ova" \
vi://vc_user_name:vc_password@vc_hostname_or_ip_address/vc_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](#)
- [Recuperarse de un error de celda en espera 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](#)
- [Aumentar la capacidad de la base de datos de PostgreSQL integrada en un 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.

Puede usar este flujo de trabajo para reutilizar las direcciones IP y el nombre de host del elemento principal con errores cuando implemente el nuevo elemento en espera.

#### Requisitos previos

- Compruebe que la celda principal se encuentra en estado inaccesible o con errores.
- Compruebe que las dos celdas en espera se encuentran en estado en ejecución.
- Familiarícese con el procedimiento para eliminar un dispositivo con errores del grupo de servidores de vCloud Director y el clúster de alta disponibilidad repmgr. Consulte la [Eliminar del registro una celda principal con errores en un clúster de alta disponibilidad de la base de datos](#).

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

#### Procedimiento

- 1 Si es posible, use la herramienta de administración de celdas para finalizar el proceso de vCloud Director. En la celda principal con errores, ejecute el siguiente comando.

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

- 2 Apague la máquina virtual principal con errores.
- 3 Inicie sesión como **raíz** en la interfaz de usuario de administración de dispositivos de una celda en espera, `https://standby_ip_address:5480`.
- 4 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.

- 5 Elimine el dispositivo principal con errores del grupo de servidores de vCloud Director y del clúster de alta disponibilidad de repmgr.
- 6 Si desea volver a utilizar la dirección IP y el nombre de host del dispositivo principal con errores, asegúrese de que este permanezca apagado o elimínelo.
- 7 Implemente un nuevo dispositivo en espera. Puede [Iniciar la implementación del dispositivo de vCloud Director](#) o [Implementar el dispositivo de vCloud Director mediante VMware OVF Tool](#).

Después de implementar el nuevo dispositivo en espera, el estado del clúster debe ser Correcto.

## Recuperarse de un error de celda en espera en un clúster de alta disponibilidad

Si una celda en espera no se ejecuta correctamente, puede recuperarse del error mediante la implementación de una nueva celda en espera.

Si una de las celdas en espera tiene el estado `Unreachable` o `Failed`, puede implementar una nueva celda. Para ver el estado de las celdas del clúster, consulte [Ver el estado de las celdas en un clúster de alta disponibilidad de la base de datos](#).

Puede usar este flujo de trabajo para reutilizar las direcciones IP y el nombre de host del elemento en espera con errores cuando implemente un nuevo elemento en espera.

- 1 Si es posible, use la herramienta de administración de celdas para finalizar el proceso de vCloud Director. En la celda en espera con errores, ejecute el siguiente comando.

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

- 2 Apague la máquina virtual en espera con errores.
- 3 Elimine el dispositivo en espera con errores del grupo de servidores de vCloud Director y del clúster de alta disponibilidad de repmgr. Consulte la [Eliminar del registro un nodo en espera con errores o inaccesible en un clúster de alta disponibilidad de la base de datos](#).
- 4 Si desea volver a utilizar la dirección IP y el nombre DNS de la celda en espera con errores, debe asegurarse de que el elemento en espera con errores permanezca apagado o eliminarlo.
- 5 Implemente un nuevo dispositivo en espera. Puede [Iniciar la implementación del dispositivo de vCloud Director](#) o [Implementar el dispositivo de vCloud Director mediante VMware OVF Tool](#).

Después de implementar el nuevo elemento en espera, el estado del clúster debe ser `Correcto`.

## 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`, `proxycertificates` y `truststore` 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.

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 vCloud Director Service Provider Admin Portal mediante la dirección IP de red de `eth0` de cualquier celda del nuevo grupo de servidores, `https://eth0_IP_new_cell/provider`.
  - b Inicie sesión en Service Provider Admin Portal 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 Service Provider Admin Portal para eliminar las celdas desconectadas que pertenezcan al entorno anterior de vCloud Director.
  - a En el menú principal () , seleccione **Recursos de nube**.
  - b En el panel izquierdo, haga clic en **Celdas de nube**.
  - c Seleccione una celda inactiva y haga clic en **Eliminar del registro**.

## 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 pg_hba.conf. Consulte <a href="#">Configurar el acceso externo a la base de datos de vCloud Director</a> .

## Aumentar la capacidad de la base de datos de PostgreSQL integrada en un dispositivo de vCloud Director

Si no dispone de espacio suficiente en el disco de la base de datos de PostgreSQL de un dispositivo de vCloud Director, puede aumentar la capacidad de la base de datos de PostgreSQL integrada.

La base de datos de PostgreSQL se encuentra en el disco duro 3. Tiene un tamaño predeterminado de 80 GB. El procedimiento se puede realizar mientras los dispositivos se encuentran en funcionamiento.

**Importante** Debe aumentar la capacidad de todos los dispositivos en espera existentes antes de aumentar la capacidad del dispositivo principal.

### Requisitos previos

- Si el entorno de vCloud Director tiene nodos en espera, identifique los nodos en espera y el nodo principal, e inicie el procedimiento desde un nodo en espera. Para obtener más información sobre cómo identificar las funciones de los nodos, consulte [Comprobar el estado de un clúster de alta disponibilidad de la base de datos](#).
- Si el entorno de vCloud Director consta únicamente de un nodo principal, ejecute el procedimiento en el nodo principal.

## Procedimiento

- 1 Inicie sesión en vSphere Client para aumentar la capacidad del disco duro 3 al tamaño que desee.

El tamaño del disco de la base de datos de PostgreSQL en cada dispositivo en espera debe ser igual al del disco de la base de datos de PostgreSQL en el dispositivo principal.

- a Seleccione la máquina virtual del dispositivo que desea modificar.
- b Seleccione **Acciones > Editar configuración**.
- c Aumente el tamaño de **Disco duro 3** y haga clic en **Aceptar**.

El progreso de la tarea de reconfiguración se mostrará en el panel **Tareas recientes**.

- 2 Aumente el tamaño lógico del volumen que utiliza la base de datos.

- a Inicie sesión directamente o utilice un cliente SSH en la consola del dispositivo de vCloud Director como **raíz**.
- b Para aplicar el cambio de tamaño del disco duro al sistema operativo, ejecute el siguiente comando.

```
echo 1 > /sys/class/scsi_device/2\:0\:2\:0/device/rescan
```

- c Para lograr que se reconozca el espacio correcto en la capa de volumen físico, ejecute el siguiente comando.

```
pvresize /dev/sdc
```

- d (opcional) Para confirmar el nuevo tamaño del volumen físico, ejecute el siguiente comando.

```
pvdisplay
```

- e Ejecute el siguiente comando para cambiar el tamaño del volumen lógico.

```
lvresize /dev/database_vg/vpostgres /dev/sdc
```

- f (opcional) Para confirmar el nuevo tamaño del volumen lógico, ejecute el siguiente comando.

```
lvdisplay
```

- 3 Aumente el tamaño del sistema de archivos para que este consuma el volumen lógico completo.

- a Para consumir el espacio adicional, ejecute el siguiente comando.

```
resize2fs /dev/database_vg/vpostgres
```

- b (opcional) Para confirmar que el sistema de archivos ha consumido el espacio adicional, ejecute `df -h`.

El espacio adicional estará disponible para el sistema operativo. La salida del sistema es similar a lo siguiente: `/dev/mapper/database_vg-vpostgres 157G 75G 82G 48% /var/vmware/vpostgres`

- 4 Si el entorno no consta de únicamente un dispositivo principal y tiene otros nodos en espera, repita los pasos 1 al 3 en todos los demás nodos en espera que tengan una base de datos y, a continuación, repita los pasos 1 al 3 en el nodo principal.

## 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](http://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.

# Referencia de la herramienta de administración de celdas

# 10

La herramienta de administración de celdas es una utilidad de línea de comandos que puede usar para administrar una base de datos o celda de vCloud Director. Se necesitan credenciales de superusuario o de administrador del sistema para realizar la mayoría de las operaciones.

La herramienta de administración de celdas se instala en `/opt/vmware/vcloud-director/bin/`. Puede utilizarla para ejecutar un único comando o bien ejecutarla como un shell interactivo.

## Lista de comandos disponibles

Para obtener una lista de los comandos de la herramienta de administración de celdas, utilice la siguiente línea de comandos.

```
./cell-management-tool -h
```

## Uso del modo de shell

Para ejecutar la herramienta de administración de celdas como un shell interactivo, invóquela sin argumentos, como se muestra a continuación.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool
Cell Management Tool v8.14.0.4146350 Type "help" for available subcommands. cmt>
```

Mientras esté en modo de shell, podrá escribir cualquier comando de la herramienta de administración de celdas en el símbolo del sistema `cmt>`, como se muestra en este ejemplo.

```
cmt>cell -h
usage: cell [options] -a,--application-states display the state of each application on the cell
[DEPRECATED - use the cell-application command instead] -h,--help print this message -i,--pid <arg>
the process id of the cell [REQUIRED if username is not specified] -m,--maintenance <arg> gracefully
enter maintenance mode on the cell -p,--password <arg> administrator password [OPTIONAL] -q,--quiesce
<arg> quiesce activity on the cell -s,--shutdown gracefully shutdown the cell -t,--status display
activity on the cell -tt,--status-verbose display a verbose description of activity on the cell -u,--
username <arg> administrator username [REQUIRED if pid is not specified] Note: You will be prompted
for administrator password if not entered in command line. cmt>
```

El comando regresa al símbolo del sistema `cmt>` cuando termina de ejecutarse. Para salir del modo de shell, escriba **exit** en el símbolo del sistema `cmt>`.

## Ejemplo: Ayuda para la utilización de la herramienta de gestión de celdas

Este ejemplo ejecuta un único comando no interactivo que enumera los comandos disponibles en la herramienta de administración del shell.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -h
usage: cell-management-tool -h,--help print this message Available commands: cell - Manipulates the
Cell and core components certificates - Reconfigures the SSL certificates for the cell . . . For
command specific help: cell-management-tool <commandName> -h
```

- **Configurar una instalación de vCloud Director**

Use el comando `system-setup` de la herramienta de administración de celdas para inicializar la base de datos del grupo de servidores con una cuenta de administrador del sistema y la información relacionada.

- **Habilitar vCloud Director Web Console**

En vCloud Director 10.0, la vCloud Director Web Console (interfaz de usuario basada en Flex) se ha vuelto obsoleta y se encuentra deshabilitada de forma predeterminada. Asimismo, la URL de Web Console redirige a las páginas de aterrizaje HTML5 correspondientes para proveedores de servicios y tenants. Puede utilizar la herramienta de administración de celdas para habilitar la Web Console.

- **Deshabilitar el acceso de proveedores de servicios al endpoint de API heredado**

A partir de vCloud Director 10.0, puede usar endpoints de inicio de sesión de OpenAPI de vCloud Director distintos para que los proveedores de servicios y los tenants accedan a vCloud Director.

- **Administrar una celda**

Con el subcomando `cell` de la herramienta de administración de celdas, es posible suspender el programador de tareas para que no se puedan iniciar nuevas tareas, ver el estado de las tareas activas, controlar el modo de mantenimiento de las celdas o apagar la celda correctamente.

- **Administrar aplicaciones de las celdas**

Utilice el comando `cell-application` de la herramienta de administración de celdas para controlar el conjunto de aplicaciones que ejecuta la celda al inicio.

- **Actualización de las propiedades de conexión de la base de datos**

Puede actualizar las propiedades de conexión de la base de datos de vCloud Director mediante el subcomando `reconfigure-database` de la herramienta de administración de celdas.

- **Detectar y reparar datos dañados del programador**

vCloud Director utiliza el programador de trabajos Quartz para coordinar las operaciones asincrónicas (trabajos) en ejecución en el sistema. Si se daña la base de datos del programador Quartz, es posible que el sistema no se pueda poner en modo inactivo correctamente. Utilice el comando `fix-scheduler-data` de la herramienta de administración de celdas para examinar la base de datos en busca de datos del programador dañados y repararlos según sea necesario.

- **Generar certificados autofirmados para los endpoints de proxy de consola y HTTP**

Utilice el comando `generate-certs` de la herramienta de administración de celdas para generar certificados SSL autofirmados para los endpoints HTTP y de proxy de consola.

- **Sustituir certificados para los endpoints de proxy de consola y HTTP**

Utilice el comando `certificates` de la herramienta de administración de celdas para sustituir los certificados SSL de los endpoints HTTP y de proxy de consola.

- **Importar certificados SSL desde servicios externos**

Utilice el comando `import-trusted-certificates` de la herramienta de administración de celdas para importar certificados que luego se usarán para establecer conexiones seguras con servicios externos, como la base de datos de vCloud Director y AMQP.

- **Administrar la lista de cifrados SSL permitidos**

Utilice el comando `ciphers` de la herramienta de administración de celdas para configurar el grupo de conjuntos de cifrado que la celda ofrece para su uso durante el proceso de protocolo de intercambio SSL.

- **Administrar la lista de protocolos SSL permitidos**

Utilice el comando `ssl-protocols` de la herramienta de administración de celdas para configurar el grupo de protocolos SSL que la celda ofrece para su uso durante el proceso de protocolo de intercambio SSL.

- **Configurar recopilación de métricas**

Utilice el comando `configure-metrics` de la herramienta de administración de celdas para configurar el conjunto de métricas que se recopilará.

- **Configurar una base de datos de métricas de Cassandra**

Utilice el comando `cassandra` de la herramienta de administración de celdas para conectar la celda con una base de datos de métricas opcional.

- **Recuperación de la contraseña del administrador del sistema**

Si conoce el nombre de usuario y la contraseña de la base de datos de vCloud Director, puede utilizar el comando `recover-password` de la herramienta de administración de celdas para recuperar la contraseña del administrador del sistema de vCloud Director.

- **Actualizar el estado de error de una tarea**

Utilice el comando `fail-tasks` de la herramienta de administración de celdas para actualizar el estado de finalización asociado con las tareas que estaban en ejecución cuando la celda se cerró deliberadamente. No puede utilizar el comando `fail-tasks` hasta que se hayan cerrado todas las celdas.

- **Configurar la administración de mensajes de auditoría**

Use el comando `configure-audit-syslog` de la herramienta de administración de celdas para configurar la forma en la que el sistema registra los mensajes de auditoría.

- **Configurar plantillas de correo electrónico**

Use el comando `manage-email` de la herramienta de administración de celdas para administrar las plantillas que usa el sistema para crear alertas de correo electrónico.

- **Encontrar máquinas virtuales huérfanas**

Use el comando `find-orphan-vm` de la herramienta de administración de celdas para encontrar referencias a las máquinas virtuales que están presentes en la base de datos de vCenter, pero no en la base de datos de vCloud Director.

- **Unirse o abandonar el Programa de mejora de la experiencia del cliente de VMware**

Para unirse al programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de VMware o abandonarlo, es posible usar el subcomando `configure-ceip` de la herramienta de administración de celdas.

- **Actualizar las opciones de configuración de la aplicación**

Con el subcomando `manage-config` de la herramienta de administración de celdas, puede actualizar diferentes opciones de configuración de la aplicación, como las actividades de limitación del catálogo.

- **Configurar la limitación de sincronización del catálogo**

Cuando tiene muchos elementos de catálogo publicados en otras organizaciones o suscritos desde estas, puede configurar la limitación de sincronización del catálogo para evitar sobrecargar el sistema durante las sincronizaciones de catálogo. Puede utilizar el subcomando `manage-config` de la herramienta de administración de celdas para configurar la regulación de sincronización del catálogo restringiendo el número de elementos de biblioteca que se pueden sincronizar al mismo tiempo.

- **Solucionar errores de acceso a la interfaz de usuario de vCloud Director**

Para ver y actualizar las entradas de DNS y las direcciones IP válidas de las celdas de vCloud Director del entorno de vCloud Director, puede utilizar el subcomando `manage-config` de la herramienta de administración de celdas.

- **Depurar la detección de máquinas virtuales de vCenter**

Mediante el uso del subcomando `debug-auto-import` de la herramienta de administración de celdas, es posible investigar el motivo por el cual el mecanismo de detección de vApps omite una o más máquinas virtuales de vCenter.



## ■ Volver a generar direcciones MAC para redes extendidas multisitio

Si asocia dos sitios de vCloud Director que están configurados con el mismo identificador de instalación, puede encontrar conflictos de direcciones MAC en redes extendidas a través de estos sitios. Para evitar este tipo de conflictos, debe volver a generar las direcciones MAC en uno de los sitios en función de una inicialización personalizada que sea diferente del identificador de instalación.

## ■ Actualizar las direcciones IP de la base de datos en celdas de vCloud Director

Puede utilizar la herramienta de administración de celdas para actualizar las direcciones IP de las celdas de vCloud Director en un clúster de alta disponibilidad de la base de datos.

# Configurar una instalación de vCloud Director

Use el comando `system-setup` de la herramienta de administración de celdas para inicializar la base de datos del grupo de servidores con una cuenta de administrador del sistema y la información relacionada.

Después de configurar todos los servidores en el grupo de servidores de vCloud Director y conectarlos con la base de datos, puede crear una cuenta de administrador del sistema inicial e inicializar la base de datos de vCloud Director con información relacionada mediante una línea de comandos del siguiente formato:

```
cell-management-tool system-setup options
```

No puede ejecutar este comando en un sistema que ya haya sido configurado. Deben especificarse todas las opciones excepto `--unattended` y `--password`.

**Tabla 10-1. Opciones y argumentos de la herramienta de administración de celdas, subcomando `system-setup`**

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--email</code>	La dirección de correo electrónico para el administrador del sistema que va a crear.	La dirección de correo electrónico del administrador del sistema se almacena en la base de datos de vCloud Director.
<code>--full-name</code>	El nombre completo del administrador del sistema que está creando.	El nombre completo del administrador del sistema se almacena en la base de datos de vCloud Director.

**Tabla 10-1. Opciones y argumentos de la herramienta de administración de celdas, subcomando `system-setup` (continuación)**

Opción	Argumento	Descripción
<code>--installation-id</code>	Un número entero del 1 al 63.	El identificador de instalación para esta instalación de vCloud Director. El sistema usa el identificador de instalación cuando se generan direcciones MAC para NIC virtuales.  <b>Nota</b> Si planea crear redes extendidas en las instalaciones de vCloud Director de una implementación multisitio, considere la posibilidad de definir un identificador de instalación único para cada instalación de vCloud Director.
<code>--password</code>	La contraseña del administrador del sistema que está creando. Es obligatoria cuando se usa la opción <code>--unattended</code> . Si no se usa la opción <code>--unattended</code> , el comando le pide esta contraseña si no la proporcionó en la línea de comandos.	El administrador del sistema proporciona esta contraseña cuando autentica en vCloud Director.
<code>--serial-number</code>	El número de serie (clave de licencia) de esta instalación.	Opcional. Debe ser un número de serie de vCloud Director válido.
<code>--system-name</code>	El nombre que debe asignarse a la carpeta de vCenter Server de vCloud Director.	Esta instalación de vCloud Director está representada por una carpeta con este nombre en cada servidor de vCenter Server con el que se registra.
<code>--unattended</code>	Ninguno	Opcional. El comando no pide más información cuando se invoca con esta opción.
<code>--user</code>	El nombre de usuario del administrador del sistema que está creando.	El administrador del sistema proporciona este nombre de usuario cuando autentica en vCloud Director.

## Ejemplo: Especificar la configuración del sistema de vCloud Director

Un comando como este especifica todos los parámetros de configuración del sistema para una nueva instalación de vCloud Director. Dado que `--unattended` y `--password` no están especificadas, el comando le pide que proporcione y confirme la contraseña que debe crear para el administrador del sistema.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool system-setup \ --user admin --
full-name "VCD System Administrator" --email vcd-admin@example.com --system-name VCD --installation-
id 2
Please enter the new password for user admin (password must have more than 6 characters):

Re-enter the password to confirm:

Username: admin
Full name: VCD System Administrator
Email: vcd-admin@example.com
System name: VCD
Installation ID: 2
Are you sure you want to use these parameters? [Y/n]:y
Creating admin user.
Setting system details.
Completing system setup.
System setup is complete.
```

## Habilitar vCloud Director Web Console

En vCloud Director 10.0, la vCloud Director Web Console (interfaz de usuario basada en Flex) se ha vuelto obsoleta y se encuentra deshabilitada de forma predeterminada. Asimismo, la URL de Web Console redirige a las páginas de aterrizaje HTML5 correspondientes para proveedores de servicios y tenants. Puede utilizar la herramienta de administración de celdas para habilitar la Web Console.

### Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo de cualquiera de las celdas de vCloud Director.
- 2 Utilice la herramienta de administración de celdas para habilitar la Web Console.
  - Para habilitar la Web Console para todos los usuarios, ejecute el siguiente comando.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n flex.ui.enabled -v true
```

- Para habilitar la Web Console solo para los administradores del sistema, ejecute el siguiente comando.

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n flex.ui.enabled -v sys-
admin-only
```

**Tabla 10-2. Opciones y argumentos de la herramienta de administración de celdas, subcomando `manage-config`**

Opción	Argumento	Descripción
<code>--name (-n)</code>	<code>flex.ui.enabled</code>	La marca para habilitar o deshabilitar la Web Console.
<code>--value (-v)</code>	<code>false</code> (valor predeterminado)	<p>El argumento <code>false</code> deshabilita la Web Console. Este es el comportamiento predeterminado.</p> <ul style="list-style-type: none"> <li>■ <code>base_cell_URL/</code> : no redirige, vuelve a cargar la página de inicio de sesión.</li> <li>■ <code>base_cell_URL/cloud:</code> redirige a <code>/provider</code>.</li> <li>■ <code>base_cell_URL/cloud/login.jsp:</code> redirige a <code>/provider</code>.</li> <li>■ <code>base_cell_URL/cloud/org/organization_name:</code> redirige a <code>/tenant/organization_name</code>.</li> </ul>
	<code>true</code>	<p>El argumento <code>true</code> habilita la Web Console.</p> <ul style="list-style-type: none"> <li>■ <code>base_cell_URL/</code> : no redirige, vuelve a cargar la página de inicio de sesión.</li> <li>■ <code>base_cell_URL/cloud:</code> no redirige.</li> <li>■ <code>base_cell_URL/cloud/login.jsp:</code> no redirige.</li> <li>■ <code>base_cell_URL/cloud/org/organization_name:</code> no redirige.</li> </ul>
	<code>sys-admin-only</code>	<p>El argumento <code>sys-admin-only</code> habilita la Web Console para los administradores del sistema.</p> <ul style="list-style-type: none"> <li>■ <code>base_cell_URL/</code> : no redirige, vuelve a cargar la página de inicio de sesión.</li> <li>■ <code>base_cell_URL/cloud:</code> no redirige.</li> <li>■ <code>base_cell_URL/cloud/login.jsp:</code> no redirige.</li> <li>■ <code>base_cell_URL/cloud/org/organization_name:</code> redirige a <code>/tenant/organization_name</code>.</li> </ul>

### 3 Reinicie la celda de vCloud Director para que se apliquen los cambios.

```
service vmware-vcd restart
```

## Pasos siguientes

- Para acceder a la vCloud Director Web Console, desplácese hasta `https://hostname.domain.tld/cloud` e inicie sesión como administrador del sistema, o desplácese hasta `https://vcloud.example.com/cloud/org/myOrg` para iniciar sesión en la organización. Para obtener más información sobre la vCloud Director Web Console, consulte la versión 9.7 de *Guía del administrador de vCloud Director* y la versión 9.7 de *Guía del usuario de vCloud Director*.
- Para deshabilitar la vCloud Director Web Console y volver a utilizar el comportamiento predeterminado, ejecute el siguiente comando.

```
cell-management-tool manage-config -n flex.ui.enabled -v false
```

## Deshabilitar el acceso de proveedores de servicios al endpoint de API heredado

A partir de vCloud Director 10.0, puede usar endpoints de inicio de sesión de OpenAPI de vCloud Director distintos para que los proveedores de servicios y los tenants accedan a vCloud Director.

vCloud Director 10.0 introduce dos nuevos endpoints de OpenAPI que puede utilizar para aumentar la seguridad mediante la restricción del acceso a vCloud Director.

- `/cloudapi/1.0.0/sessions/provider`: endpoint de OpenAPI para el inicio de sesión de proveedores de servicios. Los tenants no pueden acceder a vCloud Director mediante este endpoint.
- `/cloudapi/1.0.0/sessions/`: endpoint de OpenAPI para el inicio de sesión de tenants. Los proveedores de servicios no pueden acceder a vCloud Director mediante este endpoint.

De forma predeterminada, los administradores del proveedor y los usuarios de la organización pueden acceder a vCloud Director si inician sesión en el endpoint de API `/api/sessions`.

Con el subcomando `manage-config` de la herramienta de administración de celdas, puede deshabilitar el acceso de los proveedores de servicios al endpoint de API `/api/sessions` y, gracias a ello, limitar el inicio de sesión de los proveedores al endpoint de OpenAPI `/cloudapi/1.0.0/sessions/provider` nuevo al que solo pueden acceder los proveedores de servicios.

### Procedimiento

- 1 Inicie sesión o utilice SSH como **root** en el sistema operativo de cualquiera de las celdas de vCloud Director.
- 2 Para bloquear el acceso de los proveedores al endpoint de API `/api/sessions`, utilice la herramienta de administración de celdas y ejecute el siguiente comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n  
vcloud.api.legacy.nonprovideronly -v true
```

## Resultados

Los proveedores de servicios ya no pueden acceder al endpoint de API `/api/sessions`. Los proveedores de servicios pueden utilizar el nuevo endpoint de OpenAPI `/cloudapi/1.0.0/sessions/provider` para acceder a vCloud Director. Los tenants pueden acceder a vCloud Director mediante el endpoint de API `/api/sessions` y el nuevo endpoint de OpenAPI `/cloudapi/1.0.0/sessions/`.

## Pasos siguientes

Para habilitar el acceso de los proveedores al endpoint de API `/api/sessions`, ejecute el siguiente comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool manage-config -n
vcloud.api.legacy.nonprovideronly -v false
```

## Administrar una celda

Con el subcomando `cell` de la herramienta de administración de celdas, es posible suspender el programador de tareas para que no se puedan iniciar nuevas tareas, ver el estado de las tareas activas, controlar el modo de mantenimiento de las celdas o apagar la celda correctamente.

Para administrar celdas, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool cell -u sysadmin-username -p sysadmin-passwordoption
```

donde *sysadmin-username* y *sysadmin-password* son el nombre de usuario y la contraseña del **administrador del sistema**.

**Nota** Por motivos de seguridad, se puede omitir la contraseña. En este caso, el comando solicita que se introduzca la contraseña sin mostrarla en la pantalla.

Como alternativa para no proporcionar las credenciales del **administrador del sistema**, puede utilizar la opción `--pid` y proporcionar el identificador del proceso de la celda. Para buscar el identificador del proceso de la celda, utilice un comando similar al siguiente:

```
cat /var/run/vmware-vcd-cell.pid
```

Tabla 10-3. Opciones y argumentos de la herramienta de administración de celdas, subcomando `cell`

Opción	Argumento	Descripción
<code>--help</code> (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--pid</code> (-i)	Identificador del proceso de la celda	Puede utilizar esta opción en lugar de <code>-username</code> .

**Tabla 10-3. Opciones y argumentos de la herramienta de administración de celdas, subcomando `cell` (continuación)**

Opción	Argumento	Descripción
<code>--maintenance</code> (-m)	true o false	Establece la celda en modo de mantenimiento.  El argumento <code>true</code> pone la celda en modo inactivo y en modo de mantenimiento.  El argumento <code>false</code> libera la celda del modo de mantenimiento.
<code>--password</code> (-p)	Contraseña del <b>administrador del sistema</b> de vCloud Director	Opcional si se utiliza la opción <code>--username</code> .  Si se omite esta opción, el comando solicita que se introduzca la contraseña sin mostrarla en la pantalla.
<code>--quiesce</code> (-q)	true o false	Pone la celda en modo inactivo.  El argumento <code>true</code> suspende el programador.  El argumento <code>false</code> reinicia el programador.
<code>--shutdown</code> (-s)	Ninguno	Apaga correctamente los servicios de vCloud Director en el servidor.
<code>--status</code> (-t)	Ninguno	Muestra información en cuanto al número de tareas que se ejecutan en la celda y el estado de ésta.
<code>--status-verbose</code> (-tt)	Ninguno	Muestra información sobre el número de tareas que se ejecutan en la celda y el estado de ésta.
<code>--username</code> (-u)	Nombre de usuario del <b>administrador del sistema</b> de vCloud Director.	Puede utilizar esta opción en lugar de <code>-pid</code> .

## Administrar aplicaciones de las celdas

Utilice el comando `cell-application` de la herramienta de administración de celdas para controlar el conjunto de aplicaciones que ejecuta la celda al inicio.

vCloud Director ejecuta una serie de aplicaciones que proporcionan los servicios que requieren los clientes de vCloud Director. La celda inicia un subconjunto de estas aplicaciones de forma predeterminada. Por lo general, todos los miembros de ese subconjunto deben admitir una instalación de vCloud Director.

Para ver o modificar la lista de aplicaciones que se ejecutan al iniciar la celda, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool -u sysadmin-username -p sysadmin-password cell-application command
```

### **sysadmin-nombreUsuario**

Nombre de usuario de un administrador del sistema de vCloud Director.

### **sysadmin-contraseña**

Contraseña del administrador del sistema de vCloud Director. La contraseña debe escribirse entre comillas si contiene caracteres especiales.

**Nota** Puede proporcionar la contraseña del administrador del sistema de vCloud Director en la línea de comandos de la `cell-management-tool`, pero es más seguro omitirla. Esto hace que la `cell-management-tool` solicite la contraseña, que no se mostrará en la pantalla al escribirla.

Como alternativa a proporcionar las credenciales del administrador del sistema, puede utilizar la opción `--pid` y proporcionar el identificador del proceso de la celda. Para buscar el identificador del proceso de la celda, utilice un comando similar al siguiente:

```
cat /var/run/vmware-vcd-cell.pid
```

### **comando**

Subcomando `cell-application`.

**Tabla 10-4. Opciones y argumentos de la herramienta de administración de celdas, subcomando `cell-application`**

Comando	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--application-states</code>	Ninguno	Enumera las aplicaciones de la celda y sus estados actuales.
<code>--disable</code>	Identificador de la aplicación	Evita que esta aplicación de la celda se ejecute al iniciar la celda.
<code>--enable</code>	Identificador de la aplicación	Permite que esta aplicación de la celda se ejecute al iniciar la celda.
<code>--pid (-i)</code>	Identificador del proceso de la celda	Puede utilizar esta opción en lugar de <code>-u</code> o <code>-u</code> y <code>-p</code> .
<code>--list</code>	Ninguno	Enumera todas las aplicaciones de la celda y muestra si se ha habilitado su ejecución al iniciar la celda.
<code>--password (-p)</code>	Contraseña del administrador de vCloud Director	Opcional. El comando solicitará la contraseña si no se ha proporcionado en la línea de comandos.



**Tabla 10-4. Opciones y argumentos de la herramienta de administración de celdas, subcomando `cell-application` (continuación)**

Comando	Argumento	Descripción
<code>--set</code>	Lista de identificadores de aplicación separados por punto y coma.	Especifica el conjunto de aplicaciones de la celda que se ejecuta al iniciar la celda. Este comando sobrescribe el conjunto existente de aplicaciones de la celda que se ejecuta al iniciar la celda. Utilice <code>--enable</code> o <code>--disable</code> para cambiar el estado de inicio de una sola aplicación.
<code>--username (-u)</code>	El nombre de usuario del administrador de vCloud Director.	Es necesario si no se especifica <code>--pid</code> .

## Ejemplo: Enumerar las aplicaciones de la celda y sus estados de inicio

La siguiente línea de comandos de `cell-management-tool` requiere las credenciales del administrador del sistema, y devuelve la lista de aplicaciones de la celda y sus estados de inicio.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool -u administrator cell-
application --list
Please enter the administrator password:
```

name	id	enabled	description
Networking	com.vmware.vc...	true	Exposes NSX api endpoints directly from vCD.
Console Proxy	com.vmware.vc...	true	Proxies VM console data connection...
Cloud Proxy	com.vmware.vc...	true	Proxies TCP connections from a tenant site.
Compute Service Broker	com.vmware.vc...	true	Allows registering with a service control...
Maintenance Application	com.vmware.vc...	false	Indicates to users the cell is undergo ...
Core Cell Application	com.vmware.vc...	true	Main cell application, Flex UI and REST API.

## Actualización de las propiedades de conexión de la base de datos

Puede actualizar las propiedades de conexión de la base de datos de vCloud Director mediante el subcomando `reconfigure-database` de la herramienta de administración de celdas.

Durante la instalación de vCloud Director o el proceso de implementación del dispositivo de vCloud Director, configure las propiedades de las conexiones de base de datos y el tipo de base de datos. Consulte [Capítulo 5 Instalar vCloud Director en Linux](#) y [Capítulo 6 Implementar el dispositivo de vCloud Director](#).

Al completar la configuración de la base de datos de vCloud Director, puede actualizar las conexiones de la base de datos mediante el subcomando `reconfigure-database`. Puede mover la base de datos de vCloud Director existente a un nuevo host, cambiar el nombre de usuario y la contraseña de la base de datos, o habilitar una conexión SSL para una base de datos de PostgreSQL.

```
cell-management-tool reconfigure-database options
```

**Importante** Los cambios que se realicen al ejecutar el comando `reconfigure-database` se escribirán en el archivo de configuración global `global.properties` y el archivo de respuesta `responses.properties` de la celda. Antes de ejecutar el comando, compruebe que el archivo de respuesta esté presente en `/opt/vmware/vcloud-director/etc/responses.properties` y que se pueda editar. Para obtener información sobre la protección y la reutilización del archivo de respuesta, consulte [Capítulo 5 Instalar vCloud Director en Linux](#).

Si no utiliza la opción `--pid`, debe reiniciar la celda para aplicar los cambios.

**Tabla 10-5. Opciones y argumentos de la herramienta de administración de celdas, subcomando `reconfigure-database`**

Opción	Argumento	Descripción
<code>--help</code> ( <code>-h</code> )	Ninguno	Proporciona un resumen de las opciones disponibles en esta categoría.
<code>--database-host</code> ( <code>-dbhost</code> )	Dirección IP o nombre de dominio completo del host de base de datos de vCloud Director	Actualiza el valor de la propiedad <code>database.jdbcUrl</code> .  <b>Importante</b> El comando solo valida el formato del valor.
<code>--database-instance</code> ( <code>-dbinstance</code> )	Instancia de base de datos SQL Server	Opcional. Se usa si el tipo de base de datos es <code>sqlserver</code> .  <b>Importante</b> Si incluye esta opción, debe proporcionar el mismo valor que especificó cuando configuró la base de datos en un principio.
<code>--database-name</code> ( <code>-dbname</code> )	El nombre del servicio de base de datos.	Actualiza el valor de la propiedad <code>database.jdbcUrl</code> .
<code>--database-password</code> ( <code>-dbpassword</code> )	Contraseña para el usuario de la base de datos	Actualiza el valor de la propiedad <code>database.password</code> . La contraseña que proporciona se cifra antes de almacenarse como un valor de propiedad.

Tabla 10-5. Opciones y argumentos de la herramienta de administración de celdas, subcomando `reconfigure-database` (continuación)

Opción	Argumento	Descripción
<code>--database-port</code> ( <code>-dbport</code> )	El número de puerto usado por el servicio de base de datos en el host de base de datos.	Actualiza el valor para la propiedad <code>database.jdbcUrl</code> .  <b>Importante</b> El comando solo valida el formato del valor.
<code>--database-type</code> ( <code>-dbtype</code> )	Tipo de la base de datos. Uno de los siguientes: ■ <code>sqlserver</code> ■ <code>postgres</code>	Actualiza el valor de la propiedad <code>database.jdbcUrl</code> .
<code>--database-user</code> ( <code>-dbuser</code> )	Nombre de usuario del usuario de la base de datos	Actualiza el valor de la propiedad <code>database.user</code> .
<code>--database-ssl</code>	<code>true</code> o <code>false</code>	Se usa si el tipo de base de datos es <code>postgres</code> . Configura la base de datos de PostgreSQL para que requiera una conexión SSL desde vCloud Director.
<code>--pid</code> ( <code>-i</code> )	El identificador del proceso de la celda.	Opcional. Ejecuta una reconfiguración en caliente en una celda de vCloud Director en ejecución. No requiere el reinicio de la celda.  Si lo utiliza con <code>--private-key-path</code> , puede ejecutar el comando en celdas locales y remotas de inmediato.
<code>--private-key-path</code>	Ruta de acceso a la clave privada de la celda.	Opcional. Todas las celdas del grupo de servidores se apagan correctamente, actualizan sus propiedades de la base de datos y se reinician.  <b>Importante</b> Todas las celdas deben admitir conexiones SSH del superusuario sin una contraseña.
<code>--remote-sudo-user</code>	Un nombre de usuario con derechos <code>sudo</code> .	Se usa con la opción <code>--private-key-path</code> cuando el usuario remoto es diferente del <b>raíz</b> .  En el dispositivo, puede utilizar esta opción para el usuario <b>postgres</b> , por ejemplo, <code>--remote-sudo-user=postgres</code> .

Cuando utiliza las opciones `--database-host` y `--database-port`, el comando valida el formato de los argumentos, pero no prueba la combinación de host y puerto para la accesibilidad de red o la presencia de una base de datos en ejecución del tipo especificado.

Si utiliza la opción `--private-key-path`, todas las celdas se deben configurar para permitir conexiones SSH del superusuario sin una contraseña. Por ejemplo, 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` de 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.

## Ejemplo: Cambiar del nombre de usuario y la contraseña de la base de datos de vCloud Director

Para cambiar el nombre de usuario y la contraseña de la base de datos de vCloud Director, si deja todas las demás propiedades de conexión como se configuraron originalmente, puede ejecutar el siguiente comando:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \ --dbuser vcd-dba --dbpassword P@55w0rd
```

## Ejemplo: Actualizar la dirección IP de la base de datos de vCloud Director mediante reconfiguración en caliente en todas las celdas

Si no es un usuario raíz con derechos `sudo`, para cambiar la dirección IP de la base de datos de vCloud Director en todas las celdas de forma inmediata, puede ejecutar el siguiente comando:

```
[sudo@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool reconfigure-database \ --dbhost db_ip_address -i $(service vmware-vcd pid cell) --private-key-path=path_to_private-key \ --remote-sudo-user=non-root-user
```

## Detectar y reparar datos dañados del programador

vCloud Director utiliza el programador de trabajos Quartz para coordinar las operaciones asincrónicas (trabajos) en ejecución en el sistema. Si se daña la base de datos del programador Quartz, es posible que el sistema no se pueda poner en modo inactivo correctamente. Utilice el comando `fix-scheduler-data` de la herramienta de administración de celdas para examinar la base de datos en busca de datos del programador dañados y repararlos según sea necesario.

Para examinar las bases de datos en busca de datos dañados del programador, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool fix-scheduler-data options
```

**Tabla 10-6. Opciones y argumentos de la herramienta de administración de celdas, subcomando `fix-scheduler-data`**

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--dbuser</code>	El nombre de usuario de la base de datos de vCloud Director.	Debe proporcionarse en la línea de comandos.
<code>--dbpassword</code>	Contraseña del usuario de la base de datos de vCloud Director.	Si no se proporciona, se mostrará un indicador solicitando que se introduzca uno.

## Generar certificados autofirmados para los endpoints de proxy de consola y HTTP

Utilice el comando `generate-certs` de la herramienta de administración de celdas para generar certificados SSL autofirmados para los endpoints HTTP y de proxy de consola.

Cada grupo de servidores de vCloud Director debe admitir dos endpoints SSL: uno para el servicio HTTP y otro para el servicio de proxy de la consola. El endpoint del servicio HTTP es compatible con vCloud Director Service Provider Admin Portal, vCloud Director Tenant Portal y vCloud API. El endpoint de proxy de consola remota admite conexiones de VMRC para vApps y máquinas virtuales.

El comando `generate-certs` de la herramienta de administración de celdas automatiza el procedimiento [Crear certificados SSL autofirmados para vCloud Director en Linux](#).

Para generar certificados SSL de firma automática y añadirlos a un almacén de claves nuevo o existente, utilice una línea de comando con el siguiente formato:

```
cell-management-tool generate-certs options
```

**Tabla 10-7. Opciones y argumentos de la herramienta de administración de celdas, subcomando `generate-certs`**

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--expiration (-x)</code>	<i>días-hasta-caducidad</i>	Número de días para que caduquen los certificados. El valor predeterminado es 365.
<code>--issuer (-i)</code>	<i>nombre=valor [, nombre=valor, ...]</i>	Nombre distintivo X.509 del emisor del certificado. El valor predeterminado es <code>CN=FQDN</code> , donde <code>FQDN</code> es el nombre de dominio completo de la celda o su dirección IP si no se dispone de un nombre de dominio completo. Si especifica varios pares atributo/valor, sepárelos con comas y escriba el argumento entero entre comillas.
<code>--httpcert (-j)</code>	Ninguno	Genere un certificado para el extremo HTTP.
<code>--key-size (-s)</code>	<i>tamaño-clave</i>	Tamaño del par de claves expresado como un número entero de bits. El valor predeterminado es 2048. Los tamaños de clave inferiores a 1024 ya no se admiten según la publicación especial NIST 800-131A.
<code>--keystore-pwd (-w)</code>	<i>almacénClaves-contraseña</i>	Contraseña del almacén de claves de este host.
<code>--out (-o)</code>	<i>almacénClaves-nombreRuta</i>	Nombre de ruta completo al almacén de claves de este host.
<code>--consoleproxycert (-p)</code>	Ninguno	Genere un certificado para el extremo de proxy de consola.

**Nota** Para mantener la compatibilidad con versiones anteriores de este subcomando, omitir `-j` y `-p` da el mismo resultado que proporcionar `-j` y `-p`.

## Ejemplo: Creación de certificados de firma automática

En este ejemplo, tenemos un almacén de claves en `/tmp/cell.ks` con la contraseña `kspw`. Este almacén se va a crear si todavía no existe.

En este ejemplo, los nuevos certificados se crean con los valores predeterminados. El nombre de emisor se establece como CN=Unknown. El certificado utiliza la longitud de clave predeterminada de 2048 bits y caduca un año después de su creación.

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

En este ejemplo se genera un certificado nuevo para el extremo http únicamente. También se especifican valores personalizados para el tamaño de clave y el nombre del emisor. El nombre de emisor se establece como CN=Test, L=London, C=GB. El nuevo certificado para la conexión http tiene una clave de 4.096 bits y caduca 90 días después de su creación. El certificado existente para el extremo de proxy de consola no se ve afectado.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool generate-certs -j -o /tmp/cell.ks -w kspw -i "CN=Test, L=London, C=GB" -s 4096 -x 90
New keystore created and written to /tmp/cell.ks.
```

---

**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.

---

## Sustituir certificados para los endpoints de proxy de consola y HTTP

Utilice el comando `certificates` de la herramienta de administración de celdas para sustituir los certificados SSL de los endpoints HTTP y de proxy de consola.

El comando `certificates` de la herramienta de administración de celdas automatiza el proceso de sustitución de los certificados existentes por otros almacenados en el almacén de claves JCEKS. Utilice el comando `certificates` para sustituir certificados autofirmados por certificados firmados, o bien sustituir certificados que estén a punto de caducar por otros nuevos. Para crear un almacén de claves JCEKS que contenga certificados firmados, consulte [Crear certificados SSL autofirmados para vCloud Director en Linux](#).

Para sustituir los certificados SSL de uno o ambos endpoints, use un comando que tenga el siguiente formato:

```
cell-management-tool certificates options
```

Tabla 10-8. Opciones y argumentos de la herramienta de administración de celdas, subcomando `certificates`

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--config (-c)</code>	ruta de acceso completa al archivo <code>global.properties</code> de la celda.	De forma predeterminada, es <code>\$VCLLOUD_HOME/etc/global.properties</code> .
<code>--httpks (-j)</code>	Ninguno	Reemplace el archivo del almacén de claves denominado <code>certificates</code> que usa el endpoint <code>http</code> .
<code>--consoleproxyks (-p)</code>	Ninguno	Reemplace el archivo del almacén de claves denominado <code>proxycertificates</code> que usa el endpoint de proxy de la consola.
<code>--responses (-r)</code>	ruta de acceso completa al archivo <code>responses.properties</code>	De forma predeterminada, es <code>\$VCLLOUD_HOME/etc/responses.properties</code> .
<code>--keystore (-k)</code>	<i>almacénClaves-nombreRuta</i>	Nombre de ruta completo al almacén de claves JCEKS que contiene los certificados firmados. La forma corta y menos recomendada de <code>-s</code> ha sido sustituida por <code>-k</code> .
<code>--keystore-password (-w)</code>	<i>almacénClaves-contraseña</i>	Contraseña del almacén de claves JCEKS al que hace referencia la opción <code>--keystore</code> . Sustituye a las opciones menos recomendadas de <code>-kspassword</code> y <code>--keystorepwd</code> .

## Ejemplo: Sustitución de certificados

Podrá omitir las opciones `--config` y `--responses`, a menos que esos archivos se hayan movido de sus ubicaciones predeterminadas. En este ejemplo, un almacén de claves en `/tmp/my-new-certs.ks` tiene la contraseña `kspw`. En este ejemplo se reemplaza el certificado existente de extremo `http` de la celda por el que se ha encontrado en `/tmp/my-new-certs.ks`

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool certificates -j -k /tmp/my-new-certs.ks -w kspw
Certificate replaced by user specified keystore at /tmp/new.ks.
You will need to restart the cell for changes to take effect.
```

**Nota** Tendrá que reiniciar la celda después de sustituir los certificados.



## Importar certificados SSL desde servicios externos

Utilice el comando `import-trusted-certificates` de la herramienta de administración de celdas para importar certificados que luego se usarán para establecer conexiones seguras con servicios externos, como la base de datos de vCloud Director y AMQP.

Antes de poder realizar una conexión segura con un servicio externo, vCloud Director debe establecer una cadena válida de confianza para ese servicio. Para ello, debe importar los certificados del servicio en su propio almacén de confianza. Para importar certificados de confianza en el almacén de confianza de la celda, utilice un comando que tenga el siguiente formato:

```
cell-management-tool import-trusted-certificates options
```

**Tabla 10-9. Opciones y argumentos de la herramienta de administración de celdas, subcomando `import-trusted-certificates`**

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--destination</code>	nombre de la ruta de acceso	Nombre completo de la ruta de acceso al almacén de confianza de destino. Si no se proporciona en la línea de comandos, lo siguiente se establecerá como el valor predeterminado: <code>/opt/vmware/vcloud-director/etc/certificates</code> .
<code>--destination-password</code>	cadena	Contraseña del almacén de confianza de destino. Si no se proporciona en la línea de comandos, se usa el valor de <code>vcloud.ssl.truststore.password</code> de forma predeterminada.
<code>--destination-type</code>	tipo de almacén de claves	Tipo de almacén de claves del almacén de confianza de destino. Puede ser JKS o JCEKS. JCEKS se emplea de forma predeterminada.
<code>--force</code>	Ninguno	Reemplaza los certificados existentes en el almacén de confianza de destino.
<code>--source</code>	nombre de la ruta de acceso	Nombre completo de la ruta de acceso al archivo PEM de origen.

## Ejemplo: Importar certificados de confianza

En este ejemplo se importan los certificados de `/tmp/demo.pem` al almacén de claves local de vCloud Director en `/opt/vmware/vcloud-director/etc/certificates`. vCloud Director almacena la contraseña del almacén de claves con un formato cifrado que el comando `import-trusted-certificates` descifra.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool import-trusted-certificates --
source /tmp/demo.pem
```

## Administrar la lista de cifrados SSL permitidos

Utilice el comando `ciphers` de la herramienta de administración de celdas para configurar el grupo de conjuntos de cifrado que la celda ofrece para su uso durante el proceso de protocolo de intercambio SSL.

Cuando un cliente establece una conexión SSL con una celda vCloud Director, la celda ofrece usar solo aquellos cifrados configurados en su lista predeterminada de cifrados permitidos. Varios cifrados no se encuentran en la lista, bien porque no son lo suficientemente sólidos como para asegurar la conexión, o bien porque son conocidos por contribuir a los errores de conexión de SSL. Al instalar o actualizar vCloud Director, el script de instalación o actualización examina los certificados de la celda. Si en alguno de ellos se ha utilizado un cifrado que no se encuentra en la lista de cifrados permitidos, el script modifica la configuración de la celda para permitir el uso de dicho cifrado y muestra una advertencia. Puede seguir utilizando los certificados existentes a pesar de su dependencia de estos cifrados o puede seguir estos pasos para reemplazar los certificados y volver a configurar la lista de cifrados permitidos:

- 1 Cree nuevos certificados que no utilicen ninguno de los cifrados no permitidos. Puede usar `cell-management-tool ciphers -a` como se muestra en [Elabore la lista de todos los cifrados permitidos](#) para elaborar una lista de todos los cifrados que se permiten en la configuración predeterminada.
- 2 Utilice el comando `cell-management-tool certificates` para reemplazar los certificados existentes en la celda por los nuevos.
- 3 Utilice el comando `cell-management-tool ciphers` para volver a configurar la lista de cifrados permitidos y excluir aquellos que no se usan en los nuevos certificados. La exclusión de estos cifrados agiliza el establecimiento de una conexión SSL con la celda, ya que el número de cifrados ofrecido durante el protocolo de intercambio se reduce prácticamente al mínimo.

---

**Importante** Debido a que la consola VMRC requiere el uso de los cifrados AES256-SHA y AES128-SHA, no puede excluirlos si sus clientes vCloud Director usan la consola VMRC.

---

Para administrar la lista de cifrados SSL permitidos, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool ciphers options
```

**Tabla 10-10. Opciones y argumentos de la herramienta de administración de celdas, subcomando ciphers**

Opción	Argumento	Descripción
--help (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
--all-allowed (-a)	Ninguno	Lista de todos los cifrados permitidos.
--compatible-reset (-c)	Ninguno	Restablezca la lista predeterminada de los cifrados permitidos y permita también los cifrados que se utilizan en los certificados de esta celda.
--disallow (-d)	Lista separada por comas de nombres de cifrados, como se publica en <a href="https://www.openssl.org/docs/man1.0.2/man1/ciphers.html">https://www.openssl.org/docs/man1.0.2/man1/ciphers.html</a>	No permita los cifrados de la lista separada por comas especificada.
--list (-l)	Ninguno	Lista de los cifrados actualmente permitidos.
--reset (-r)	Ninguno	Restablezca la lista predeterminada de los cifrados permitidos. Si los certificados de esta celda utilizan cifrados no permitidos, no podrá establecer una conexión SSL con la celda hasta que instale los nuevos certificados con un cifrado permitido.

## Ejemplo: Elabore la lista de todos los cifrados permitidos

Use la opción `--all-allowed (-a)` para elaborar una lista de todos los cifrados que se permiten actualmente en la celda para su uso durante un protocolo de intercambio SSL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -a
* TLS_DHE_DSS_WITH_AES_256_CBC_SHA
* TLS_DHE_DSS_WITH_AES_128_CBC_SHA
* TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
* TLS_DHE_RSA_WITH_AES_256_CBC_SHA
* TLS_DHE_RSA_WITH_AES_128_CBC_SHA
* TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_RSA_WITH_AES_256_CBC_SHA
* TLS_RSA_WITH_AES_128_CBC_SHA
* TLS_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
```

```
* TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_256_CBC_SHA
* TLS_ECDH_RSA_WITH_AES_128_CBC_SHA
* TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_RSA_WITH_3DES_EDE_CBC_SHA
* SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

## Ejemplo: No permita dos cifrados

Use la opción `--disallow (-d)` para quitar uno o varios cifrados de la lista de cifrados permitidos. Esta opción requiere un nombre de cifrado como mínimo. Puede proporcionar varios nombres de cifrados en una lista separada por comas. Puede obtener los nombres para esta lista de la salida de `ciphers -a`. En este ejemplo se quitan dos cifrados incluidos en el ejemplo anterior.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ciphers -d
SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA,SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
```

## Administrar la lista de protocolos SSL permitidos

Utilice el comando `ssl-protocols` de la herramienta de administración de celdas para configurar el grupo de protocolos SSL que la celda ofrece para su uso durante el proceso de protocolo de intercambio SSL.

Cuando un cliente establece una conexión SSL con una celda vCloud Director, la celda ofrece usar solo aquellos protocolos configurados en su lista de protocolos SSL permitidos. Algunos protocolos, incluidos TLSv1, SSLv3 y SSLv2Hello no se encuentran en la lista predeterminada, ya que se sabe que tienen graves vulnerabilidades de seguridad.

Para administrar la lista de protocolos SSL permitidos, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool ssl-protocols options
```

**Tabla 10-11. Opciones y argumentos de la herramienta de administración de celdas, subcomando `ssl-protocols`**

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--all-allowed (-a)</code>	Ninguno	Elabore una lista de todos los protocolos SSL que admite vCloud Director.

Tabla 10-11. Opciones y argumentos de la herramienta de administración de celdas, subcomando `ssl-protocols` (continuación)

Opción	Argumento	Descripción
<code>--disallow (-d)</code>	Lista separada por comas de nombres de protocolos SSL.	Vuelva a configurar la lista de protocolos SSL no permitidos con los que se especifican en la lista.
<code>--list (-l)</code>	Ninguno	Elabore una lista de protocolos SSL permitidos que admita la configuración actual de vCloud Director.
<code>--reset (-r)</code>	Ninguno	Restablecer los valores de fábrica de la lista de protocolos SSL configurados

**Importante** Debe reiniciar la celda después de ejecutar `ssl-protocols --disallow` o `ssl-protocols reset`.

## Ejemplo: Elaborar una lista de los protocolos SSL permitidos y configurados

Use la opción `--all-allowed (-a)` para elaborar una lista de todos los protocolos SSL que se pueden permitir en la celda para su uso durante un protocolo de intercambio SSL.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -a
Product default SSL protocols:

* TLSv1.2
* TLSv1.1
* TLSv1
* SSLv3
* SSLv2Hello
```

Esta lista suele ser un directorio de protocolos SSL que la configuración de la celda admite. Para elaborar una lista de dichos protocolos SSL, utilice la opción `--list (-l)`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -l
Allowed SSL protocols:

* TLSv1.2
* TLSv1.1
```

## Ejemplo: Volver a configurar la lista de protocolos SSL no permitidos

Utilice la opción `--disallow (-d)` para volver a configurar la lista de protocolos SSL no permitidos. Esta opción requiere una lista separada por comas del subconjunto de protocolos permitidos producida por `ssl-protocols -a`.

En este ejemplo se actualiza la lista de protocolos SSL permitidos con el fin de incluir TLSv1. Las versiones de VMware® vCenter™ anteriores a 5.5 Update 3e requieren TLSv1.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool ssl-protocols -d SSLv3,SSLv2Hello
```

Debe reiniciar la celda después de ejecutar este comando.

## Configurar recopilación de métricas

Utilice el comando `configure-metrics` de la herramienta de administración de celdas para configurar el conjunto de métricas que se recopilará.

vCloud Director puede recopilar métricas que ofrecen información actual e histórica sobre el rendimiento y consumo de recursos de las máquinas virtuales. Utilice este subcomando para configurar las métricas que recopila vCloud Director. Utilice el subcomando `cell-management-tool cassandra` para configurar una base de datos de Apache Cassandra y emplearla como repositorio de métricas de vCloud Director. Consulte [Configurar una base de datos de métricas de Cassandra](#).

Para configurar las métricas que recopila vCloud Director, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool configure-metrics --metrics-config pathname
```

**Tabla 10-12. Opciones y argumentos de la herramienta de administración de celdas, subcomando `configure-metrics`**

Comando	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--repository-host</code> (obsoleto)	Nombre de host o dirección IP del host de KairosDB	Obsoleto. Utilice la opción <code>--cluster-nodes</code> del subcomando <code>cell-management-tool cassandra</code> para configurar una base de datos de Apache Cassandra y emplearla como repositorio de métricas de vCloud Director.
<code>--repository-port</code> (obsoleto)	Puerto de KairosDB que se va a usar.	Obsoleto. Utilice la opción <code>--port</code> del subcomando <code>cell-management-tool cassandra</code> para configurar una base de datos de Apache Cassandra y emplearla como repositorio de métricas de vCloud Director.
<code>--metrics-config</code>	nombre de la ruta de acceso	Ruta al archivo de configuración de métricas.

## Ejemplo: Configuración de una conexión de la base de datos de métricas

En este ejemplo se configura la recopilación de métricas tal como se especifica en el archivo `/tmp/metrics.groovy`.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool configure-metrics --metrics-config /tmp/metrics.groovy
```

El servicio de recopilación de métricas de vCloud Director implementa un subconjunto de las métricas recopiladas por vSphere Performance Manager. Consulte la documentación de vSphere Performance Manager para obtener más información sobre los nombres de métrica y los parámetros de recopilación. El archivo `metrics-config` menciona uno o varios nombres de métrica y proporciona parámetros de recopilación para cada métrica mencionada. Por ejemplo:

```
configuration {
    metric("cpu.usage.average")
    metric("cpu.usagemhz.average")
    metric("cpu.usage.maximum")
    metric("disk.used.latest") {
        currentInterval=300
        historicInterval=300
        entity="VM"
        instance=""
        minReportingInterval=1800
        aggregator="AVERAGE"
    }
}
```

A continuación se enumeran los nombres de métrica admitidos.

Tabla 10-13. Nombres de métrica

Nombre de métrica	Descripción
<code>cpu.usage.average</code>	Vista de host del promedio de uso activo de CPU de esta máquina virtual como porcentaje del total disponible. Incluye todos los núcleos de todos los sockets.
<code>cpu.usagemhz.average</code>	Vista de host del promedio de uso activo de CPU de esta máquina virtual como medida sin formato. Incluye todos los núcleos de todos los sockets.
<code>cpu.usage.maximum</code>	Vista de host del uso máximo activo de CPU de esta máquina virtual como porcentaje del total disponible. Incluye todos los núcleos de todos los sockets.
<code>mem.usage.average</code>	Memoria utilizada por esta máquina virtual como porcentaje del total de memoria configurada.
<code>disk.provisioned.latest</code>	Espacio de almacenamiento asignado a este disco duro virtual en el centro de datos virtual de la organización en la que se encuentra.
<code>disk.used.latest</code>	Almacenamiento utilizado por todos los discos duros virtuales.

Tabla 10-13. Nombres de métrica (continuación)

Nombre de métrica	Descripción
disk.read.average	Promedio de velocidad de lectura de todos los discos duros virtuales.
disk.write.average	Promedio de velocidad de escritura de todos los discos duros virtuales.

**Nota** Cuando una máquina virtual tiene varios discos, las métricas se muestran como una suma de todos los discos. Las métricas de CPU son una suma de todos los núcleos y los sockets.

Se pueden especificar los siguientes parámetros de recopilación para cada métrica con nombre.

Tabla 10-14. Parámetros de recopilación de métricas

Nombre de parámetro	Valor	Descripción
currentInterval	Número entero de segundos.	El intervalo en segundos que se utiliza al consultar los valores de métrica más recientes disponibles (para consultas de métricas actuales). El valor predeterminado es 20 si no se ha especificado. Los valores superiores a 20 solo se admiten para métricas de nivel 1, tal como define vSphere Performance Manager.
historicInterval	Número entero de segundos.	El intervalo en segundos que se utiliza al consultar los valores históricos de métrica. El valor predeterminado es 20 si no se ha especificado. Los valores superiores a 20 solo se admiten para métricas de nivel 1, tal como define vSphere Performance Manager.
entity	Uno de: HOST, VM	El tipo de objeto de VC para el que está disponible la métrica. El valor predeterminado es Máquina virtual si no se ha especificado. No todas las métricas están disponibles para todas las entidades.
instance	Un identificador de instancia de PerfMetricId de vSphere Performance Manager.	Indica si se deben recuperar datos de las instancias individuales de una métrica (por ejemplo, núcleos de CPU individuales), una agregación de todas las instancias o ambas. Un valor de "*" recopila todas las métricas, la instancia y la agregación. Una cadena vacía, "", solo recopila los datos agregados. Una cadena específica (como "DISKFILE") solo recopila datos para esa instancia. El valor predeterminado es "*" si no se ha especificado.
minReportingInterval	Número entero de segundos.	Especifica un intervalo de agregación predeterminado en segundos para usarlo cuando se creen informes de datos de series temporales. Proporciona más control sobre la granularidad de los informes cuando la granularidad del intervalo de recopilación no es suficiente. El valor predeterminado es 0 (sin intervalo de informes dedicado).
aggregator	Uno de los siguientes: AVERAGE, MINIMUM, MAXIMUM o SUMMATION	El tipo de agregación que se realiza durante minReportingInterval. El valor predeterminado es AVERAGE si no se ha especificado.



## Configurar una base de datos de métricas de Cassandra

Utilice el comando `cassandra` de la herramienta de administración de celdas para conectar la celda con una base de datos de métricas opcional.

vCloud Director puede recopilar métricas que ofrecen información actual e histórica sobre el rendimiento y consumo de recursos de las máquinas virtuales. Utilice este subcomando para configurar una base de datos de Apache Cassandra y emplearla como repositorio de métricas de vCloud Director. Utilice el subcomando `cell-management-tool configure-metrics` para configurar el grupo de métricas que desea recopilar. Consulte [Configurar recopilación de métricas](#).

Los datos de métricas históricas se almacenan en una base de datos de Apache Cassandra. Consulte [Instalar y configurar una base de datos de Cassandra para almacenar datos de métricas históricas](#) para obtener más información acerca de cómo configurar el software de base de datos opcional para almacenar y recuperar las métricas de rendimiento.

Para crear una conexión entre vCloud Director y una base de datos de Apache Cassandra, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool cassandra options
```

**Tabla 10-15. Opciones y argumentos de la herramienta de administración de celdas, subcomando `cassandra`**

Comando	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de las opciones disponibles para este comando.
<code>--add-rollup</code>	Ninguno	Actualiza el esquema de métricas para incluir métricas acumuladas. Consulte la <a href="#">Instalar y configurar una base de datos de Cassandra para almacenar datos de métricas históricas</a> .
<code>--cluster-nodes</code>	<i>dirección</i> [, <i>dirección</i> ... ]	Lista separada por comas de los nodos del clúster de Cassandra que se va a utilizar para las métricas de vCloud Director.
<code>--clean</code>	Ninguno	Se quitan las opciones de configuración de Cassandra de la base de datos de vCloud Director.
<code>--configure</code>	Ninguno	Se configura vCloud Director para usarlo con un clúster de Cassandra existente.
<code>--dump</code>	Ninguno	Se vuelca la configuración de conexión actual.

**Tabla 10-15. Opciones y argumentos de la herramienta de administración de celdas, subcomando `cassandra` (continuación)**

Comando	Argumento	Descripción
<code>--keyspace</code>	cadena	El nombre del espacio de claves de vCloud Director en Cassandra se establece en <i>cadena</i> . De forma predeterminada, es <code>vcloud_metrics</code> .
<code>--offline</code>	Ninguno	Cassandra se configura para que la use vCloud Director, pero no se prueba la configuración mediante la conexión a vCloud Director.
<code>--password</code>	cadena	Contraseña del usuario de la base de datos de Cassandra.
<code>--port</code>	entero	Puerto para conectarse a cada nodo del clúster. El valor predeterminado es 9042.
<code>--ttl</code>	entero	Se conservan los datos de métricas para los días <i>enteros</i> . <i>entero</i> se establece en 0 para que los datos de métricas se conserven para siempre.
<code>--update-schema</code>	Ninguno	Inicializa el esquema de Cassandra para retener los datos de métricas de vCloud Director.
<code>--username</code>	cadena	Nombre de usuario del usuario de la base de datos de Cassandra.

## Ejemplo: Configuración de una conexión de la base de datos de Cassandra

Utilice un comando como este, donde *node1-ip*, *node2-ip*, *node3-ip* y *node4-ip* sean la dirección 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 'P@55w0rd' --ttl 15
```

Debe reiniciar la celda una vez que se complete este comando.

## Recuperación de la contraseña del administrador del sistema

Si conoce el nombre de usuario y la contraseña de la base de datos de vCloud Director, puede utilizar el comando `recover-password` de la herramienta de administración de celdas para recuperar la contraseña del administrador del sistema de vCloud Director.

Con el comando `recover-password` de la herramienta de administración de celdas, un usuario que conozca el nombre de usuario y la contraseña de la base de datos de vCloud Director puede recuperar la contraseña del administrador del sistema de vCloud Director.

Para recuperar la contraseña del administrador del sistema, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool recover-password options
```

**Tabla 10-16. Opciones y argumentos de la herramienta de administración de celdas, subcomando `recover-password`**

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--dbuser</code>	El nombre de usuario de la base de datos de vCloud Director.	Debe proporcionarse en la línea de comandos.
<code>--dbpassword</code>	Contraseña del usuario de la base de datos de vCloud Director.	Si no se proporciona, se mostrará un indicador solicitando que se introduzca uno.

## Actualizar el estado de error de una tarea

Utilice el comando `fail-tasks` de la herramienta de administración de celdas para actualizar el estado de finalización asociado con las tareas que estaban en ejecución cuando la celda se cerró deliberadamente. No puede utilizar el comando `fail-tasks` hasta que se hayan cerrado todas las celdas.

Cuando pone una celda en modo inactivo con el comando `cell-management-tool -q`, las tareas en ejecución finalizan en unos minutos. Si una tarea sigue en ejecución en una celda que ha sido puesta en modo inactivo, el superusuario puede cerrar la celda, lo que fuerza el error en todas las tareas en ejecución. Después de un cierre que fuerce el error de las tareas en ejecución, el superusuario puede ejecutar `cell-management-tool fail-tasks` para actualizar el estado de finalización de dichas tareas. Actualizar el estado de finalización de una tarea de esta forma es opcional pero ayuda a mantener la integridad de los registros del sistema al identificar con claridad los errores causados por una acción administrativa.

Para generar una lista de tareas en ejecución en una celda que se ha puesto en modo inactivo, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool -u sysadmin-nombreUsuario cell --status-verbose
```

Tabla 10-17. Opciones y argumentos de la herramienta de administración de celdas, subcomando `fail-tasks`

Comando	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--message (-m)</code>	Texto del mensaje.	Texto del mensaje para el estado de finalización de tarea.

## Ejemplo: Error de las tareas que se ejecutan en la celda

Este ejemplo actualiza el estado de finalización de la tarea asociado con la tarea que estaba en ejecución cuando la celda fue cerrada.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool fail-tasks -m "administrative shutdown"
Operation: IMPORT_SINGLETON_VAPP, Start time: 12/16/13 6:41 PM, Username: system, Organization: org1
Would you like to fail the tasks listed above?
```

Escriba **y** para actualizar la tarea con un estado de finalización de **cierre administrativo**.

Escriba **n** para permitir que la tarea continúe ejecutándose.

**Nota** Si se devuelven varias tareas como respuesta, debe decidir si todas deben dar error o no hacer nada. No puede elegir un subgrupo de tareas que dé error.

## Configurar la administración de mensajes de auditoría

Use el comando `configure-audit-syslog` de la herramienta de administración de celdas para configurar la forma en la que el sistema registra los mensajes de auditoría.

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` de Linux además de a la base de datos de vCloud Director.

El script de configuración del sistema permite especificar el modo en que se administran los mensajes de auditoría. Consulte "Configurar conexiones de red y de base de datos" en la *Guía de instalación y actualización de vCloud Director*. Las opciones de registro que especifique durante la configuración del sistema se conservan en dos archivos: `global.properties` y `responses.properties`. Puede cambiar la configuración de registro de los mensajes de auditoría en ambos archivos con una línea de comandos de la herramienta de administración de celdas con el siguiente formato:

```
cell-management-tool configure-audit-syslog options
```

Todos los cambios que realice con este subcomando de la herramienta de administración de celdas se conservan en los archivos `global.properties` y `responses.properties` de la celda. Los cambios no surten efecto hasta que se reinicie la celda.

**Tabla 10-18. Opciones y argumentos de la herramienta de administración de celdas, subcomando `configure-audit-syslog`**

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--disable (-d)</code>	Ninguno	Desactiva el registro de los eventos de auditoría en <code>syslog</code> . Registra los eventos de auditoría solamente en la base de datos de vCloud Director. Esta opción anula la configuración de los valores de las propiedades <code>audit.syslog.host</code> y <code>audit.syslog.port</code> en <code>global.properties</code> y <code>responses.properties</code> .
<code>--syslog-host (-loghost)</code>	Dirección IP o nombre de dominio completo del host del servidor Syslog	Esta opción configura el nombre de dominio completo o la dirección especificada como el valor de la propiedad <code>audit.syslog.host</code> .
<code>--syslog-port (-logport)</code>	Entero dentro del rango 0-65535	Esta opción configura el entero especificado como el valor de la propiedad <code>audit.syslog.port</code> .

Al especificar un valor para `--syslog-host` o `--syslog-port` (o ambas), el comando valida que el valor especificado tenga la forma correcta, pero no prueba la combinación de host y puerto para comprobar la accesibilidad de red o la presencia de un servicio de `syslog` en ejecución.

## Ejemplo: Cambiar el nombre de host del servidor Syslog

**Importante** Los cambios que realice usando este comando se escriben en el archivo de configuración global y en el archivo de respuesta. Antes de utilizar este comando, asegúrese de que el archivo de respuesta está en su lugar (en `/opt/vmware/vcloud-director/etc/responses.properties`) y se puede escribir en él. Consulte "Protección y reutilización del archivo de respuesta" en la *Guía de instalación y actualización de vCloud Director*.

Para cambiar el host al que se envían los mensajes de Syslog, use un comando como el siguiente:

```
[root@cell1 /opt/vmware/vcloud-director/bin]# cell-management-tool configure-audit-syslog -loghost
syslog.example.com
Using default port 514
```

En este ejemplo se supone que el nuevo host escucha mensajes de Syslog en el puerto predeterminado.

El comando actualiza `global.properties` y `responses.properties`, pero los cambios no entran en efecto hasta que reinicie la celda.

## Configurar plantillas de correo electrónico

Use el comando `manage-email` de la herramienta de administración de celdas para administrar las plantillas que usa el sistema para crear alertas de correo electrónico.

De manera predeterminada, el sistema está configurado para enviar alertas de correo electrónico que notifican a los administradores del sistema eventos y condiciones que puede que requieran su intervención. La lista de destinatarios de correo electrónico puede actualizarse con la consola web o la API de vCloud. Puede reemplazar el contenido de correo electrónico predeterminado para cada tipo de alerta mediante el uso de una línea de comandos de la herramienta de administración de celdas con el siguiente formato:

```
cell-management-tool manage-email options
```

**Tabla 10-19. Opciones y argumentos de la herramienta de administración de celdas, subcomando `manage-email`**

Opción	Argumento	Descripción
<code>--help</code>	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--delete</code>	Nombre de la plantilla	El nombre de la plantilla por eliminar.
<code>--lookup</code>	Nombre de la plantilla	Este argumento es opcional. Si no lo proporciona, el comando devuelve una lista de todos los nombres de plantilla.
<code>--locale</code>	La configuración regional de la plantilla	De manera predeterminada, este comando utiliza plantillas de la configuración regional en-US. Use esta opción para especificar una configuración regional diferente.
<code>--set-template</code>	Nombre de la ruta de acceso a un archivo con una plantilla de correo electrónico actualizada	Se debe poder acceder a este archivo en el host local y el usuario <code>vcloud.vcloud</code> debe poder leerlo. Por ejemplo, <code>/tmp/my-email-template.txt</code>

## Ejemplo: Actualizar una plantilla de correo electrónico

El siguiente comando reemplaza el contenido actual de la plantilla de correo electrónico DISK\_STORAGE\_ALERT\_VDCS con contenido creado en un archivo llamado /tmp/DISK\_STORAGE\_ALERT\_VDCS-new.txt.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-email --set-template
DISK_STORAGE_ALERT_VDCS /tmp/DISK_STORAGE_ALERT_VDCS-new.txt

New property being stored: Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value
"This is an alert from $productName The $datastore is used by the following PVDC(s): $pvdcList
"

Property "email.template.DISK_STORAGE_ALERT_VDCS.en-US" has value "This is an alert from $productName
The $datastore is used by the followingProvider VDC(s): $pvdcList
"

VCD Email notification details:
name                : DISK_STORAGE_ALERT_VDCS
description         : Alert when used disk storage exceeds threshold
config key          : email.template.DISK_STORAGE_ALERT_VDCS.en-US
template placeholders : [productName, storageContainerType, datastore, percentage,
currentFreeSpaceMB, diskSizeBytes, pvdcList]
template content    : This is an alert from $productName The $datastore is used by the
followingProvider VDC(s): $pvdcList
```

## Encontrar máquinas virtuales huérfanas

Use el comando `find-orphan-vms` de la herramienta de administración de celdas para encontrar referencias a las máquinas virtuales que están presentes en la base de datos de vCenter, pero no en la base de datos de vCloud Director.

Las máquinas virtuales a las que se hace referencia en la base de datos de vCenter, pero no en la base de datos de vCloud Director, se consideran máquinas virtuales huérfanas porque vCloud Director no puede acceder a ellas aunque estén usando recursos informáticos y de almacenamiento. Este tipo de incoherencia en la referencia puede deberse a varias razones, entre las cuales se encuentran cargas de trabajo de volumen alto, errores en bases de datos y acciones administrativas. El comando `find-orphan-vms` permite a un administrador enumerar estas máquinas virtuales para que puedan quitarse o volver a importarse en vCloud Director. Su comando tiene medidas de contingencia para especificar un almacén de confianza alternativo, que puede necesitarse si está trabajando con instalaciones de vCloud Director o vCenter que usan certificados autofirmados.

Utilice un comando con el siguiente formato:

```
cell-management-tool find-orphan-vms options
```

**Tabla 10-20. Opciones y argumentos de la herramienta de administración de celdas, subcomando find-orphan-vm**

Opción	Argumento	Descripción
--help (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
--enableVerifyHostname	Ninguno	Active la parte de verificación del nombre de host del protocolo de enlace de SSL.
--host	Obligatorio	La dirección IP o el nombre de dominio completo de la instalación de vCloud Director para buscar máquinas virtuales huérfanas.
--output-file	Nombre de la ruta de acceso o -	Nombre completo de la ruta de acceso del archivo en el que debe escribirse la lista de máquinas virtuales huérfanas. Especifique un nombre de ruta de acceso de - para escribir la lista en la salida estándar.
--password (-p)	Obligatorio	Contraseña del administrador del sistema de vCloud Director.
--port	Puerto HTTPS de vCloud Director	Especifique esto solamente si no quiere que este comando use el puerto HTTPS predeterminado de vCloud Director.
--trustStore	Nombre completo de la ruta de acceso al archivo del almacén de confianza de Java	Especifique esto solamente si no quiere que este comando use el archivo del almacén de confianza predeterminado de vCloud Director.
--trustStorePassword	Contraseña para la opción --trustStore especificada	Obligatoria solo si usa --trustStore para especificar un archivo de almacén de confianza alternativo.
--trustStoreType	El tipo de opción --trustStore especificada (PKCS12, JCEKS, etc.)	Obligatoria solo si usa --trustStore para especificar un archivo de almacén de confianza alternativo.
--user (-u)	Obligatorio	Nombre de usuario del administrador del sistema de vCloud Director.
--vc-name	Obligatorio	Nombre de vCenter para buscar máquinas virtuales huérfanas.



Tabla 10-20. Opciones y argumentos de la herramienta de administración de celdas, subcomando `find-orphan-vms` (continuación)

Opción	Argumento	Descripción
<code>--vc-password</code>	Obligatorio	Contraseña del administrador de vCenter.
<code>--vc-user</code>	Obligatorio	Nombre de usuario del administrador de vCenter.

## Ejemplo: Encontrar máquinas virtuales huérfanas

En este ejemplo se consulta a un solo servidor de vCenter Server. Debido a que `--output-file` se especifica como `-`, los resultados se devuelven en la salida estándar.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./cell-management-tool find-orphan-vms \
--host 10.20.30.40 -u vadmin -vc-name vcenter1 -vc-password P055w0rd --vc-user admin --output-file -
Querying for VC by name 10.20.30.40
Querying all vdc's associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc<->resource pool mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Querying all vdc<->VM Moref mappings associated with VC: 10.20.30.40 (https://10.20.30.40:443)
Processing 956 VM's on 5 VDC's across 20 resource pools
Analysis complete.
VDC: "ExampleOrgVDC [urn:vcloud:vdc:1a97...]" (org: "ExampleOrg") ResPool: primary (1a97...) [moref:
"resgroup-30515"]
The following 22 orphan VMs were discovered:
Orphan VM: "indDisk100-0-95411 (cbc358a0-e199-4024-8fff-2e5cfce20953)" (parent name: "Test VMs",
parent moref : "group-v30533")
...
Orphan VM: "indDisk12-0-51259 (0bbb4115-673e-4c84-ba26-6875159655e0)" (parent name: "Test VMs",
parent moref : "group-v30533")
```

## Unirse o abandonar el Programa de mejora de la experiencia del cliente de VMware

Para unirse al programa de mejora de la experiencia de cliente (Customer Experience Improvement Program, CEIP) de VMware o abandonarlo, es posible usar el subcomando `configure-ceip` de la herramienta de administración de celdas.

Este producto forma parte del Programa de mejora de la experiencia del cliente de VMware (CEIP). 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.

```
cell-management-tool
configure-ceip
options
```

Si prefiere no participar en el CEIP de VMware para este producto, ejecute este comando con la opción `--disable`.

**Tabla 10-21. Opciones y argumentos de la herramienta de administración de celdas, subcomando `configure-ceip`**

Opción	Argumento	Descripción
<code>--help</code> ( <code>-h</code> )	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--disable</code>	Ninguno	Abandona el programa de mejora de la experiencia de cliente de VMware.
<code>--enable</code>	Ninguno	Se une al programa de mejora de la experiencia de cliente de VMware.
<code>--status</code>	Ninguno	Muestra el estado de participación actual en el programa de mejora de la experiencia de cliente de VMware.

## Ejemplo: Abandonar el programa de mejora de la experiencia de cliente de VMware

Para abandonar el programa de mejora de la experiencia de cliente de VMware, use un comando similar al siguiente:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
disableParticipation disabled
```

Después de ejecutarlo, el sistema ya no enviará información al Programa de mejora de la experiencia del cliente de VMware.

Para confirmar el estado de participación actual en el programa de mejora de la experiencia de cliente de VMware, use un comando similar al siguiente:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#cell-management-tool configure-ceip --
statusParticipation disabled
```

## Actualizar las opciones de configuración de la aplicación

Con el subcomando `manage-config` de la herramienta de administración de celdas, puede actualizar diferentes opciones de configuración de la aplicación, como las actividades de limitación del catálogo.

**Tabla 10-22. Opciones y argumentos de la herramienta de administración de celdas, subcomando `manage-config`**

Opción	Argumento	Descripción
<code>--help (-h)</code>	Ninguno	Proporciona un resumen de las opciones disponibles con este subcomando.
<code>--delete (-d)</code>	Ninguno	Quita la opción de configuración de destino.
<code>--lookup (-l)</code>	Ninguno	Busca el valor de la opción de configuración de destino.
<code>--name (-n)</code>	Nombre de la opción de configuración	El nombre de la opción de configuración de destino. Es obligatorio con las opciones <code>-d</code> , <code>-l</code> y <code>-v</code> .
<code>--value (-v)</code>	Valor de la opción de configuración	Agrega o actualiza el valor de la opción de configuración de destino.

Por ejemplo, puede utilizar el subcomando `manage-config` para [Configurar la limitación de sincronización del catálogo](#).

## Configurar la limitación de sincronización del catálogo

Cuando tiene muchos elementos de catálogo publicados en otras organizaciones o suscritos desde estas, puede configurar la limitación de sincronización del catálogo para evitar sobrecargar el sistema durante las sincronizaciones de catálogo. Puede utilizar el subcomando `manage-config` de la herramienta de administración de celdas para configurar la regulación de sincronización del catálogo restringiendo el número de elementos de biblioteca que se pueden sincronizar al mismo tiempo.

Cuando un catálogo suscrito inicia una sincronización de catálogo, el catálogo publicado descarga los elementos de biblioteca desde el repositorio de vCenter Server en el almacenamiento de servicio de transferencia de vCloud Director y, a continuación, crea vínculos de descarga para el catálogo suscrito. Puede limitar el número de elementos de biblioteca que todos los catálogos publicados pueden descargar al mismo tiempo. Puede limitar el número de elementos de biblioteca que todos los catálogos suscritos pueden sincronizar al mismo tiempo. Puede limitar el número de elementos de biblioteca que un solo catálogo suscrito puede sincronizar al mismo tiempo.

Puede utilizar el subcomando `manage-config` de la herramienta de administración de celdas para actualizar la configuración de la limitación del catálogo. Para obtener información sobre el uso del subcomando `manage-config`, consulte [Actualizar las opciones de configuración de la aplicación](#).

Tabla 10-23. Opciones de configuración de la limitación del catálogo

Opciones de configuración	Valor predeterminado	Descripción
<code>vcloud.tasks.VDC_ENABLE_DOWNLOAD.queue.limit</code>	30	El límite de elementos de biblioteca que todos los catálogos publicados en la instancia de vCloud Director pueden descargar de vCenter Server a vCloud Director al mismo tiempo. Si el número total de elementos de biblioteca publicados que se descargarán en la instancia de vCloud Director supera este límite, los elementos de biblioteca se dividen en partes según dicho límite y se descargan de manera secuencial.
<code>vcloud.tasks.LIBRARY_ITEM_SYNC.queue.limit</code>	30	El límite de elementos de biblioteca que todos los catálogos suscritos en una instancia de vCloud Director pueden sincronizar al mismo tiempo. Si el número total de elementos de biblioteca suscritos que se sincronizarán en la instancia de vCloud Director supera este límite, los elementos se dividen en partes según dicho límite y se sincronizan de manera secuencial.
<code>contentLibrary.item.sync.batch.size</code>	10	El límite de elementos de biblioteca que un solo catálogo suscrito puede sincronizar al mismo tiempo. Si un catálogo suscrito intenta sincronizar un número de elementos de biblioteca que supera este límite, los elementos se dividen en partes según dicho límite y se sincronizan de manera secuencial.

## Ejemplo: Configurar la limitación de sincronización para los catálogos suscritos

El siguiente comando establece un límite de cinco para los elementos de biblioteca que un solo catálogo suscrito puede sincronizar al mismo tiempo.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n
contentLibrary.item.sync.batch.size -v 5
```

Si un catálogo suscrito contiene 13 elementos de biblioteca, la sincronización del catálogo se realiza en tres partes secuenciales. La primera parte contiene cinco elementos, la segunda contiene los siguientes cinco elementos y la última contiene los tres elementos restantes.

## Solucionar errores de acceso a la interfaz de usuario de vCloud Director

Para ver y actualizar las entradas de DNS y las direcciones IP válidas de las celdas de vCloud Director del entorno de vCloud Director, puede utilizar el subcomando `manage-config` de la herramienta de administración de celdas.

### Problema

No se puede acceder al vCloud Director Service Provider Admin Portal ni al vCloud Director Tenant Portal después de iniciar sesión correctamente.

Después de introducir las credenciales en la pantalla de inicio de sesión, se muestra el siguiente mensaje de error: No se ha podido iniciar. Se detectó un error durante la inicialización. Esto puede deberse a problemas como el acceso a la aplicación a través de una URL pública no admitida o una baja conectividad.

### Causa

vCloud Director emplea una implementación de filtro de Uso compartido de recursos de origen cruzado (Cross-Origin Resource Sharing, CORS) para gestionar una lista de todos los endpoints válidos que puede utilizar para acceder al Service Provider Admin Portal y al vCloud Director Tenant Portal.

La lista de filtrado de CORS se rellena y se actualiza durante la configuración de celdas. Contiene entradas HTTP y HTTPS con direcciones IP y nombres DNS para todas las celdas del grupo de servidores. Asimismo, contiene una dirección IP pública que utiliza el equilibrador de carga que se encuentra por delante del grupo de servidores de vCloud Director.

Durante la configuración de celdas de las implementaciones de dispositivos, la lista no se actualiza con los nombres DNS de las celdas de vCloud Director y no puede utilizar el nombre DNS de una celda para acceder a ella.

### Solución

- 1 Inicie sesión o utilice SSH como **raíz** en una de las celdas del grupo de servidores.
- 2 Para obtener una lista de las URL válidas que puede utilizar para acceder a las celdas de vCloud Director del entorno, ejecute la siguiente línea de comandos.

```
[root@cell /opt/vmware/vcloud-director/bin]#./cell-management-tool manage-config -n  
webapp.allowed.origins -l
```

La salida del sistema es una lista que contiene entradas HTTP y HTTPS con direcciones IP y nombres DNS para todas las celdas del grupo de servidores. Asimismo, contiene una dirección IP pública que utiliza el equilibrador de carga que se encuentra por delante del grupo de servidores de vCloud Director.

La lista es una cadena separada por comas y sin espacios entre las entradas.

- 3 (opcional) Para actualizar la opción de configuración `webapp.allowed.origins`, ejecute la línea de comandos que se muestra más adelante. En la línea de comandos, el parámetro de valor de la opción es una lista de direcciones IP y nombres DNS en una cadena separada por comas sin espacios entre las entradas.

```
[root@cell /opt/vmware/vcloud-director/bin]# ./cell-management-tool manage-config -n
webapp.allowed.origins -v "comma_separated_list_of_URLs_without_spaces"
```

## Depurar la detección de máquinas virtuales de vCenter

Mediante el uso del subcomando `debug-auto-import` de la herramienta de administración de celdas, es posible investigar el motivo por el cual el mecanismo de detección de vApps omite una o más máquinas virtuales de vCenter.

En la configuración predeterminada, un VDC de organización detecta automáticamente las máquinas virtuales de vCenter que se crean en los grupos de recursos que respaldan al VDC. Consulte el tema sobre cómo detectar y adoptar información de vApps en la *Guía del portal para administradores de proveedores de servicios de vCloud Director*. Si una máquina virtual de vCenter no aparece en una vApp detectada, puede ejecutar el subcomando `debug-auto-import` para esa máquina virtual o ese VDC.

```
cell-management-tool debug-auto-import options
```

El subcomando `debug-auto-import` devuelve una lista de las máquinas virtuales de vCenter e información sobre los posibles motivos por los cuales el mecanismo de detección las omite. La lista también incluye las máquinas virtuales de vCenter que se detectaron, pero que no se pudieron importar al VDC de la organización.

**Tabla 10-24. Opciones y argumentos de la herramienta de administración de celdas, subcomando `debug-auto-import`**

Opción	Argumento	Descripción
<code>--help</code> (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--org</code>	Nombre de la organización	Opcional. Muestra información sobre las máquinas virtuales omitidas de la organización especificada.
<code>--vm</code>	Nombre de máquina virtual o parte de un nombre de máquina virtual	Muestra información sobre las máquinas virtuales omitidas que contienen el nombre de máquina virtual especificado. Opcional si se utiliza la opción <code>--org</code> .

## Ejemplo: test de depuración de detección de máquinas virtuales de vCenter por nombre de máquina virtual

El siguiente comando devuelve información sobre las máquinas virtuales de vCenter omitidas en todas las organizaciones.

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool debug-auto-import -vm test
```

```
VM with name:vm22-test (09ad258c-0cb0-4f69-a0a6-201cf3fe7d6b), moref vm-50 in VC testbed-vc can be skipped for the following reasons:
```

- 1) Virtual machine is already imported in vCD or is managed by vCD
- 2) Virtual machine is created by vCD

```
VM with name:test-vm1 (32210d0d-ef64-4637-b1d6-6400743a6bd9), moref vm-44 in VC testbed-vc can be skipped for the following reasons:
```

- 1) Virtual machine is not present in a vCD managed resource pool

```
VM with name:import-test3, moref vm-52inVC testbed-vc can be skippedforthe following reasons:
```

- 1) Virtual machine autoimport is either pending,in-progress or has failed and pendingforretry

En este ejemplo, el resultado del sistema devuelve información sobre tres máquinas virtuales de vCenter omitidas por el mecanismo de detección y cuyos nombres contienen la cadena test. La máquina virtual import-test3 es un ejemplo de máquina virtual detectada que no se ha importado al VDC.

## Volver a generar direcciones MAC para redes extendidas multisitio

Si asocia dos sitios de vCloud Director que están configurados con el mismo identificador de instalación, puede encontrar conflictos de direcciones MAC en redes extendidas a través de estos sitios. Para evitar este tipo de conflictos, debe volver a generar las direcciones MAC en uno de los sitios en función de una inicialización personalizada que sea diferente del identificador de instalación.

Durante la configuración inicial de vCloud Director, debe establecer un identificador de instalación. vCloud Director utiliza el identificador de instalación para generar direcciones MAC para las interfaces de red de máquina virtual. Dos instalaciones de vCloud Director que estén configuradas con el mismo identificador de instalación podrían generar direcciones MAC idénticas. Las direcciones MAC duplicadas podrían causar conflictos en redes extendidas entre dos sitios asociados.

Antes de crear redes extendidas entre sitios asociados que están configurados con el mismo identificador de instalación, debe volver a generar las direcciones MAC en uno de los sitios mediante el subcomando mac-address-management de la herramienta de administración de celdas.

```
cell-management-tool mac-address-management options
```

Para generar nuevas direcciones MAC, debe establecer una inicialización personalizada que sea diferente del identificador de instalación. La inicialización no sobrescribe el identificador de instalación, pero la base de datos almacena la inicialización más reciente como un segundo parámetro de configuración, lo que anula el identificador de instalación.

El subcomando `mac-address-management` se ejecuta desde un miembro de vCloud Director arbitrario del grupo de servidores. El comando se ejecuta en la base de datos de vCloud Director, por lo que debe ejecutar el comando una vez por cada grupo de servidores.

**Importante** La regeneración de direcciones MAC requiere cierto tiempo de inactividad de vCloud Director. Antes de comenzar la regeneración, debe poner en modo inactivo las actividades en todas las celdas del grupo de servidores.

**Tabla 10-25. Opciones y argumentos de la herramienta de administración de celdas, subcomando `mac-address-management`**

Opción	Argumento	Descripción
<code>--help</code> (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
<code>--regenerate</code>	Ninguno	Elimina todas las direcciones MAC que no estén en uso y genera direcciones MAC nuevas en función de la inicialización actual. Si no hay ninguna inicialización previamente configurada, las direcciones MAC se vuelven a generar en función del identificador de instalación. Se conservan las direcciones MAC en uso.

**Nota** Todas las celdas del grupo de servidores deben estar inactivas. Para obtener información sobre cómo poner en modo inactivo las actividades en una celda, consulte [Administrar una celda](#).



Tabla 10-25. Opciones y argumentos de la herramienta de administración de celdas, subcomando `mac-address-management` (continuación)

Opción	Argumento	Descripción
<code>--regenerate-with-seed</code>	Un número de inicialización entre 0 y 63	<p>Establece una nueva inicialización personalizada en la base de datos, elimina todas las direcciones MAC que no están en uso y genera direcciones MAC nuevas en función de la inicialización recién establecida. Se conservan las direcciones MAC en uso.</p> <hr/> <p><b>Nota</b> Todas las celdas del grupo de servidores deben estar inactivas. Para obtener información sobre cómo poner en modo inactivo las actividades en una celda, consulte <a href="#">Administrar una celda</a>.</p>
<code>--show-seed</code>	Ninguno	Devuelve la inicialización actual y el número de direcciones MAC que están en uso para cada inicialización.

**Importante** Se conservan las direcciones MAC en uso. Para cambiar una dirección MAC en uso por una dirección MAC regenerada, debe restablecer la dirección MAC de la interfaz de red. Para obtener información sobre cómo editar las propiedades de máquina virtual, consulte *Guía del portal para tenants de vCloud Director*.

## Ejemplo: Volver a generar direcciones MAC en función de una inicialización personalizada nueva

El siguiente comando establece la inicialización actual como 9 y vuelve a generar todas las direcciones MAC que no están en uso en función de la inicialización recién establecida:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --regenerate-with-seed 9
Successfully removed 65,535 unused MAC addresses.
Successfully generated new MAC addresses.
```

## Ejemplo: Visualizar la inicialización actual y el número de direcciones MAC en uso para cada inicialización

El siguiente comando devuelve información sobre la inicialización actual y el número de direcciones MAC por inicialización:

```
[root@cell1 /opt/vmware/vcloud-director/bin]#./cell-management-tool mac-address-management --show-seed
Current MAC address seed is '9' and based on MacAddressSeed config.
MAC address seed    9 is in use by    12 MAC addresses
MAC address seed    1 is in use by     1 MAC addresses
```

En este ejemplo, el resultado del sistema muestra que la inicialización actual es 9 y hay 12 direcciones MAC que se basan en ella. Además, hay una dirección MAC que se basa en una inicialización o un identificador de instalación anteriores igual a 1.

## Actualizar las direcciones IP de la base de datos en celdas de vCloud Director

Puede utilizar la herramienta de administración de celdas para actualizar las direcciones IP de las celdas de vCloud Director en un clúster de alta disponibilidad de la base de datos.

### Requisitos previos

Si desea actualizar las direcciones IP de las celdas en un clúster de alta disponibilidad de la base de datos, debe proporcionar la dirección IP del nodo principal actual. Para buscar la dirección IP, compruebe el estado del clúster para determinar el nodo que tiene la función principal. Es preciso que el nodo esté en ejecución. En esa fila, utilice el valor de host de la columna Cadena de conexión para identificar la dirección IP. 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 las celdas del clúster.
- 2 Compruebe si la celda se está ejecutando en ese nodo.

```
service vmware-vcd pid cell
```

Si el identificador de proceso de la celda no es nulo, la celda de vCloud Director se está ejecutando y se puede cambiar la dirección IP de la base de datos sin tener que reiniciar la celda de vCloud Director.

- 3 Para actualizar las direcciones IP en todas las celdas del grupo de servidores, ejecute el siguiente comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address --pid cell process ID --remote-sudo-user postgres --private-key-path /opt/vmware/vcloud-director/id_rsa
```

Los resultados del sistema indican que la reconfiguración se ha realizado correctamente.

- 4 (opcional) Compruebe si cada celda de vCloud Director apunta a la dirección IP de la base de datos correcta.

```
grep "database.jdbcUrl" /opt/vmware/vcloud-director/etc/global.properties
```

Los resultados del sistema indican que la celda está actualizada.

- 5 Si alguna de las celdas no se actualiza, ejecute el comando para volver a configurarla.

- Si la celda no se está ejecutando, ejecute el siguiente comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address
```

- Si la celda se está ejecutando, ejecute el siguiente comando:

```
/opt/vmware/vcloud-director/bin/cell-management-tool reconfigure-database --database-host primary node IP address -i cell process ID
```

- 6 Si ha vuelto a configurar una celda que no está en ejecución, ejecute el comando para reiniciar el servicio de vmware-vcd.

- a Ejecute el comando para detener el servicio.

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

- b Ejecute el comando para iniciar el servicio.

```
systemctl start vmware-vcd
```

# Después de instalar vCloud Director o implementar el dispositivo de vCloud Director

# 11

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.

Después de crear el dispositivo de vCloud Director, puede utilizar las funciones de redes de vSphere para agregar una nueva tarjeta de interfaz de red (NIC). Consulte la información [Agregar un adaptador de red a una máquina virtual](#) en la guía *Administrar máquinas virtuales de vSphere*.

Este capítulo incluye los siguientes temas:

- [Instalar archivos de Microsoft Sysprep en los servidores](#)
- [Cambiar la zona horaria del dispositivo de vCloud Director](#)
- [Personalizar direcciones públicas](#)
- [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 11-1. 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.

## Cambiar la zona horaria del dispositivo de vCloud Director

Después de implementar correctamente el dispositivo de vCloud Director, puede cambiar la zona horaria del sistema del dispositivo. Todas las instancias del dispositivo de vCloud Director del

grupo de servidores y del almacenamiento de servidores de transferencia deben utilizar la misma configuración.

#### Requisitos previos

- Implemente el dispositivo de vCloud Director. Consulte la [Capítulo 6 Implementar el dispositivo de vCloud Director](#).
- Cambie la zona horaria del almacenamiento de servidores de transferencia a la nueva zona horaria del dispositivo de vCloud Director principal.

#### Procedimiento

- 1 En la parte inferior izquierda de la ventana de una consola web o una consola remota del nodo principal, seleccione **Establecer zona horaria**.
- 2 Seleccione una ubicación, un país y una región de zona horaria.  
  
La zona horaria recién seleccionada aparece en la parte inferior izquierda de la ventana de la consola.
- 3 Inicie sesión en la consola del dispositivo de vCloud Director como **raíz**.
- 4 Para garantizar que el dispositivo de vCloud Director utiliza la nueva zona horaria, reinicie el servicio `vmware-vcd`.
- 5 Repita las instrucciones del [paso 1](#) al [Paso 4](#) para las celdas de aplicación y en espera de la implementación de vCloud Director.

## Personalizar direcciones públicas


Para satisfacer los requisitos de equilibrador de carga o proxy, puede cambiar las direcciones web de endpoint predeterminadas para vCloud Director Web Portal, vCloud API 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 [Paso 6](#).

#### Requisitos previos

Solo el **administrador del sistema** puede personalizar endpoints públicos.

#### Procedimiento

- 1 En el menú principal () , seleccione **Administración**.
- 2 En el panel izquierdo, en **Configuración**, haga clic en **Direcciones públicas**.
- 3 Haga clic en **Editar** para personalizar los endpoints públicos.

**4** Para personalizar las URL de vCloud Director, edite los endpoints de **Web Portal**.

- a Introduzca una URL pública de vCloud Director personalizada para las conexiones HTTP (no seguras).
- b Introduzca una URL pública de vCloud Director personalizada para las conexiones HTTPS (seguras) y haga clic en **Cargar** para cargar los certificados que establecen la cadena de confianza de ese endpoint.

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 `consoleproxy`. No se admite la terminación SSL de conexiones de proxy de la consola en un equilibrador de carga. 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** (opcional) Para personalizar la API de REST de vCloud y las URL de OpenAPI, desactive el botón de alternancia **Usar la configuración de Web Portal**.

- 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 **Cargar** 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.

**6** 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.

---

Por ejemplo, para una instancia de dispositivo de vCloud Director con el FQDN `vcloud.example.com`, introduzca **`vcloud.example.com:8443`**.

vCloud Director utiliza la dirección de proxy de la consola al abrir una ventana de consola remota en una máquina virtual.

7 Para guardar los cambios, haga clic en **Guardar**.

## 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 'P@55w0rd' --ttl 15
```

Para obtener información sobre el uso de la herramienta de administración de celdas, consulte [Capítulo 10 Referencia de la herramienta de administración de celdas](#).

- 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 'P@55w0rd'
```

- 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 [Capítulo 10 Referencia de la herramienta de administración de celdas](#).

### 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.

# Actualización de vCloud Director

# 12

Para actualizar vCloud Director a una nueva versión, debe apagar los servicios de vCloud Director en todas las celdas del grupo de servidores, instalar la nueva versión en cada servidor, actualizar la base de datos de vCloud Director y reiniciar las celdas 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 a un dispositivo de vCloud Director 10.0. Consulte [Capítulo 13 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 a una versión más reciente del dispositivo de vCloud Director. Utilice el instalador de vCloud Director de Linux para actualizar el entorno existente solo como parte del flujo de trabajo de migración. Consulte [Migrar al dispositivo de vCloud Director](#).

Para las instalaciones de vCloud Director en Linux, puede realizar una actualización organizada, o bien actualizar de forma manual vCloud Director. Consulte [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.

Para la actualización del dispositivo de vCloud Director de la versión 9.7 a la versión 10.0, consulte [Actualizar el dispositivo de vCloud Director](#).

A partir de vCloud Director 9.5:

- Las bases de datos de Oracle no son compatibles. Si la instalación de vCloud Director existente utiliza una base de datos de Oracle, consulte la tabla [Rutas de actualización y migración](#).
- No se permite habilitar ni deshabilitar hosts ESXi. Antes de iniciar la actualización, debe habilitar todos los hosts ESXi. Puede colocar los hosts ESXi en modo de mantenimiento mediante vSphere 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>.

A partir de vCloud Director 10.0, no se admiten las bases de datos de Microsoft SQL Server.

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. Para obtener más información, consulte la tabla Rutas de actualización y migración.
- La versión de VMware vSphere® en uso.
- La versión de VMware NSX® en uso.
- Todos los componentes de terceros que interactúan directamente con vCloud Director.

Para obtener información sobre 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](http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php).

Si tiene pensado actualizar componentes de vSphere o NSX como parte de la actualización de vCloud Director, deberá actualizarlos después de actualizar vCloud Director. Consulte [Capítulo 14 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*.

## Flujos de trabajo y rutas de actualización y migración

Entorno de origen	Entorno de destino	
	vCloud Director 10.0 en Linux con una base de datos de PostgreSQL externa	Dispositivo de vCloud Director 10.0 con una base de datos de PostgreSQL integrada
vCloud Director 9.0 y 9.1 con una base de datos de Oracle externa	<ol style="list-style-type: none"> <li>1 Para vCloud Director 9.0 en Linux, actualice vCloud Director a la versión 9.1. Consulte <a href="#">Actualización de vCloud Director</a>.</li> <li>2 Migre la base de datos de Oracle a una base de datos de PostgreSQL. Consulte <a href="#">Migrar a una base de datos de PostgreSQL</a>.</li> <li>3 Actualice el entorno a vCloud Director 10.0 en Linux. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> o <a href="#">Actualizar manualmente una instalación de vCloud Director</a>.</li> </ol>	<ol style="list-style-type: none"> <li>1 Para vCloud Director 9.0 en Linux, actualice vCloud Director a la versión 9.1. Consulte <a href="#">Actualización de vCloud Director</a>.</li> <li>2 Migre la base de datos de Oracle a una base de datos de PostgreSQL. Consulte <a href="#">Migrar a una base de datos de PostgreSQL</a>.</li> <li>3 Actualice el entorno a vCloud Director 10.0 en Linux. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> o <a href="#">Actualizar manualmente una instalación de vCloud Director</a>.</li> <li>4 Migre al dispositivo de vCloud Director 10.0. Consulte <a href="#">Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director</a>.</li> </ol>
Dispositivo de vCloud Director 9.5 con una base de datos de PostgreSQL externa	No compatible	<ol style="list-style-type: none"> <li>1 Actualice el entorno a vCloud Director 10.0 en Linux. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> o <a href="#">Actualizar manualmente una instalación de vCloud Director</a>.</li> <li>2 Migre al dispositivo de vCloud Director 10.0. Consulte <a href="#">Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director</a>.</li> </ol>
vCloud Director 9.0, 9.1 y 9.5 en Linux con una base de datos de PostgreSQL externa	Actualice el entorno a vCloud Director 10.0 en Linux. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> o <a href="#">Actualizar manualmente una instalación de vCloud Director</a> .	<ol style="list-style-type: none"> <li>1 Actualice el entorno a vCloud Director 10.0 en Linux. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> o <a href="#">Actualizar manualmente una instalación de vCloud Director</a>.</li> <li>2 Migre al dispositivo de vCloud Director 10.0. Consulte <a href="#">Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director</a>.</li> </ol>

Entorno de origen	Entorno de destino	
	vCloud Director 10.0 en Linux con una base de datos de PostgreSQL externa	Dispositivo de vCloud Director 10.0 con una base de datos de PostgreSQL integrada
vCloud Director 9.0, 9.1 y 9.5 en Linux con una base de datos externa de Microsoft SQL Server	<ol style="list-style-type: none"> <li>1 Actualice el entorno a vCloud Director 9.7 en Linux. Consulte <a href="#">Actualización de vCloud Director</a>.</li> <li>2 Migre la base de datos de Microsoft SQL Server a una base de datos de PostgreSQL. Consulte <a href="#">Migrar a una base de datos de PostgreSQL</a>.</li> <li>3 Actualice el entorno a vCloud Director 10.0 en Linux. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> o <a href="#">Actualizar manualmente una instalación de vCloud Director</a>.</li> </ol>	<ol style="list-style-type: none"> <li>1 Actualice el entorno a vCloud Director 9.7 en Linux. Consulte <a href="#">Actualización de vCloud Director</a>.</li> <li>2 Migre al dispositivo de vCloud Director 9.7. Consulte <a href="#">Migración de vCloud Director con una base de datos externa de Microsoft SQL al dispositivo de vCloud Director</a>.</li> <li>3 Actualice el entorno al dispositivo de vCloud Director 10.0. Consulte <a href="#">Actualizar el dispositivo de vCloud Director</a>.</li> </ol>
vCloud Director 9.7 en Linux con una base de datos externa de Microsoft SQL Server	<ol style="list-style-type: none"> <li>1 Migre la base de datos de Microsoft SQL Server a una base de datos de PostgreSQL. Consulte <a href="#">Migrar a una base de datos de PostgreSQL</a>.</li> <li>2 Actualice el entorno a vCloud Director 10.0 en Linux. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> o <a href="#">Actualizar manualmente una instalación de vCloud Director</a>.</li> </ol>	<ol style="list-style-type: none"> <li>1 Migre al dispositivo de vCloud Director 9.7. Consulte <a href="#">Migración de vCloud Director con una base de datos externa de Microsoft SQL al dispositivo de vCloud Director</a>.</li> <li>2 Actualice el entorno al dispositivo de vCloud Director 10.0. Consulte <a href="#">Actualizar el dispositivo de vCloud Director</a>.</li> </ol>
vCloud Director 9.7 en Linux con una base de datos de PostgreSQL externa	Actualice el entorno a vCloud Director 10.0 en Linux. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> o <a href="#">Actualizar manualmente una instalación de vCloud Director</a> .	<ol style="list-style-type: none"> <li>1 Migre al dispositivo de vCloud Director 9.7. Consulte <a href="#">Migración de vCloud Director con una base de datos de PostgreSQL externa al dispositivo de vCloud Director</a>.</li> <li>2 Actualice el entorno al dispositivo de vCloud Director 10.0. Consulte <a href="#">Actualizar el dispositivo de vCloud Director</a>.</li> </ol>
Dispositivo de vCloud Director 9.7 con una base de datos de PostgreSQL integrada	No compatible	Actualice el entorno al dispositivo de vCloud Director 10.0. Consulte <a href="#">Actualizar el dispositivo de vCloud Director</a> .
vCloud Director 10.0 en Linux con una base de datos de PostgreSQL externa	N/D	Migre al dispositivo de vCloud Director 10.0. Consulte <a href="#">Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director</a> .

Este capítulo incluye los siguientes temas:

- [Actualizar el dispositivo de vCloud Director](#)
- [Revertir un dispositivo de vCloud Director a la versión anterior cuando se produce un error en una actualización](#)
- [Actualizar el dispositivo de vCloud Director mediante el repositorio de actualizaciones de VMware](#)
- [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](#)

## Actualizar el dispositivo de vCloud Director

Puede actualizar el dispositivo de vCloud Director de la versión 9.7 a la versión 10.0 o actualizar vCloud Director 10.0 a una versión de revisión.

Mientras se actualiza 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 actualizar 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 actualización a cada dispositivo de vCloud Director y después de que se complete la actualización de la base de datos, debe reiniciar cada dispositivo de vCloud Director.

### Requisitos previos

Realice una instantánea del dispositivo de vCloud Director principal.

- 1 Inicie sesión en la instancia de vCenter Server en la que reside el dispositivo de vCloud Director principal del clúster de alta disponibilidad de la base de datos.
- 2 Desplácese hasta el dispositivo de vCloud Director principal, haga clic con el botón derecho en él y, a continuación, haga clic en **Alimentación > Desconectar SO invitado**.
- 3 Haga clic con el botón derecho en el dispositivo y haga clic en **Instantáneas > Realizar instantánea**. Introduzca un nombre y, si lo desea, una descripción para la instantánea. Después, haga clic en **Siguiente**.
- 4 Haga clic con el botón derecho en el dispositivo de vCloud Director y haga clic en **Alimentación > Encender**.
- 5 Compruebe que todos los nodos de la configuración de alta disponibilidad de la base de datos estén en buen estado. Consulte la [Comprobar el estado de un clúster de alta disponibilidad de la base de datos](#).

## 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 actualizar el dispositivo principal antes que las celdas en espera y de aplicación. Debe usar el dispositivo principal al realizar una copia de seguridad de la base de datos.

- 2 Descargue el paquete de actualización en el dispositivo que se va a actualizar.

---

**Nota** Primero debe actualizar el dispositivo principal.

---

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_10.0.0.4424-14420378_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 actualización aparece como una actualización disponible.

- 7 Ejecute el siguiente comando para apagar vCloud Director:

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

- 8 Aplique la actualización disponible.

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

- 9 Repita 2 a 8 en las celdas restantes en espera y de aplicación.

- 10 En el dispositivo principal, realice una copia de seguridad de la base de datos integrada del dispositivo de vCloud Director.

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



- 11 En cualquier dispositivo, ejecute la utilidad upgrade de la base de datos de vCloud Director.

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

- 12 Reinicie cada dispositivo de vCloud Director.

```
shutdown -r now
```

#### Pasos siguientes

- Si la actualización se realiza correctamente, puede eliminar la instantánea del dispositivo de vCloud Director.
- Si, por el contrario, la actualización no se realiza correctamente, puede revertir el dispositivo de vCloud Director a la instantánea que realizó antes de la actualización. Consulte la [Revertir un dispositivo de vCloud Director a la versión anterior cuando se produce un error en una actualización](#).

## Revertir un dispositivo de vCloud Director a la versión anterior cuando se produce un error en una actualización

Si se produce un error en la actualización de un dispositivo de vCloud Director, puede utilizar la instantánea del dispositivo que realizó antes de la actualización para revertir este dispositivo de vCloud Director a la versión anterior.

Antes de comenzar la reversión, complete el procedimiento que se describe en [Comprobar el estado de un clúster de alta disponibilidad de la base de datos](#). Tome nota de los identificadores de nodo de los nodos en espera del clúster.

- 1 Revierta el dispositivo de vCloud Director principal a la instantánea que realizó antes de iniciar la actualización.

Consulte cómo restaurar instantáneas de máquinas virtuales mediante las opciones de reversión. Consulte [Restaurar instantáneas de máquina virtual mediante la reversión](#) en *Guía de administración de máquinas virtuales de vSphere*.

- 2 Encienda la celda del dispositivo de vCloud Director principal.
- 3 Inicie sesión directamente o mediante un cliente SSH en el SO de cada celda del dispositivo de vCloud Director. Debe iniciar sesión como usuario **raíz**.
- 4 Detenga los servicios de vCloud Director en todas las celdas del dispositivo.

```
service vmware-vcd stop
```

- 5 Utilice la celda principal de vCloud Director para eliminar el registro de los nodos secundarios en el clúster.
  - a Inicie sesión directamente o mediante un cliente SSH en el SO de la celda principal como **raíz**.

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

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

- c Ejecute el comando para eliminar el registro de una celda del dispositivo en espera.

Para cancelar del registro un nodo en espera que no está en ejecución, debe proporcionar el identificador del nodo.

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

- d Repita [5.c](#) para eliminar el registro de la otra celda del dispositivo en espera.

- 6 En vSphere Client, apague y elimine todos los dispositivos en espera.

- En vSphere Client, desplácese hasta los dispositivos en espera.
- Haga clic con el botón derecho en un dispositivo en espera y haga clic en **Alimentación > Desconectar SO invitado**.
- Haga clic con el botón derecho en el dispositivo y haga clic en **Eliminar del disco**.
- Repita los pasos [6.a](#) a [6.c](#) para la otra celda del dispositivo en espera.

- 7 Compruebe que el conjunto de herramientas de repmgr y la base de datos de PostgreSQL integrada de la celda del dispositivo de vCloud Director principal funcionen correctamente.

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

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

- b Ejecute el comando para ver el estado del clúster.

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

Los resultados de la consola muestran información sobre el único nodo del clúster.

ID	Name	Role	Status	Upstream	Location	Connection string
Node 1	Nombre de nodo	primary	*running			default   host=dirección IP del host user=repmgr dbname=repmgr

- Vuelva a implementar los dispositivos secundarios. Consulte la [Implementar el dispositivo de vCloud Director mediante vSphere Client](#).
- Inicie sesión directamente o mediante un cliente SSH en el SO de cada celda del dispositivo de vCloud Director. Debe iniciar sesión como usuario **raíz**.
- Inicie los servicios de vCloud Director.

```
service vmware-vcd start
```

# Actualizar el dispositivo de vCloud Director mediante el repositorio de actualizaciones de VMware

Puede utilizar el repositorio de actualizaciones de VMware para actualizar el dispositivo de vCloud Director de la versión 9.7 a la versión 10.0.

---

**Nota** Puede utilizar el repositorio de actualización de VMware solo para actualizar vCloud Director a la versión de vCloud Director más reciente. Solo la versión más reciente está disponible en el repositorio de actualización de VMware. Si desea actualizar vCloud Director a una versión diferente, consulte [Actualizar el dispositivo de vCloud Director](#).

---

Mientras se actualiza 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 actualizar 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 actualización a cada dispositivo de vCloud Director y después de que se complete la actualización de la base de datos, debe reiniciar cada dispositivo de vCloud Director.

## Requisitos previos

Compruebe que el dispositivo de vCloud Director tenga acceso a `https://vapp-updates.vmware.com`.

## 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 usar el dispositivo principal al realizar una copia de seguridad de la base de datos.

- 2 Restablezca el repositorio de actualizaciones para que apunte al repositorio de actualización de VMware.

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

- 3 Compruebe si existen actualizaciones para verificar si el repositorio de actualizaciones de VMware tiene la actualización deseada.

De forma predeterminada, el comando `vamcli` apunta al repositorio de actualizaciones de VMware.

```
vamcli update --check
```

La versión de la actualización aparece como una actualización disponible.

- 4 Ejecute el siguiente comando para apagar vCloud Director:

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

- 5 Aplique la actualización disponible.

```
vamcli update --install latest
```

- 6 Repita el proceso desde el [Paso 2](#) hasta el [Paso 4](#) en cada dispositivo.
- 7 En el dispositivo principal, realice una copia de seguridad de la base de datos integrada del dispositivo de vCloud Director.

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

- 8 En cualquier dispositivo, ejecute la utilidad `upgrade` de la base de datos de vCloud Director.

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

- 9 Reinicie cada dispositivo de vCloud Director.

```
shutdown -r now
```

## 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 grupo 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 13 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 o una base de datos de Microsoft SQL Server, compruebe que se haya realizado la migración a una base de datos de PostgreSQL antes de actualizar a la versión 10.0 de vCloud Director. Para conocer las posibles rutas de actualización, consulte [Capítulo 12 Actualización de vCloud Director](#).

---

- 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 archivo-de-instalación
```

- 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 grupo 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 13 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 ejecutar una actualización organizada de la instalación de vCloud Director. Consulte [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 o una base de datos de Microsoft SQL Server, compruebe que se haya realizado la migración a una base de datos de PostgreSQL antes de actualizar a la versión 10.0 de vCloud Director. Para conocer las posibles rutas de actualización, consulte [Capítulo 12 Actualización de vCloud Director](#).

---

- 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.
- [Actualizar cada instancia de NSX Manager que esté asociada con un sistema vCenter Server adjunto](#)
- Después de actualizar cada NSX Manager, puede actualizar los sistemas vCenter Server, los hosts y las instancias de Edge de NSX. Consulte [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 archivo-de-instalación
```

**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
<b>Si no ha cambiado las propiedades de registro existentes</b>	Copie este archivo en <code>/opt/vmware/vcloud-director/etc/log4j.properties</code> .
<b>Si ha cambiado las propiedades de registro</b>	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 no actualizadas no se pueden conectar a la base de datos. Debe actualizar todas las celdas para que puedan conectarse 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 [Capítulo 10 Referencia de la herramienta de administración de celdas](#).
- Revise el tema [Referencia de la utilidad de actualización de bases de datos](#).

## 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.

La ubicación de la utilidad `upgrade` es `/opt/vmware/vcloud-director/bin/`.

**Tabla 12-1. Argumentos y opciones de la utilidad de actualización de bases de datos**

Opción	Argumento	Descripción
<code>--backup-completed</code>	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.
<code>--ceip-user</code>	El nombre de usuario para la cuenta de servicio del CEIP.	Si ya existe un usuario con este nombre de usuario en la organización del sistema, se producirá un error en la actualización. Predeterminado: <code>phone-home-system-account</code> .
<code>--enable-ceip</code>	<p>Elija uno:</p> <ul style="list-style-type: none"> <li>■ <code>true</code></li> <li>■ <code>false</code></li> </ul>	Especifica si esta instalación participa en el Programa de mejora de la experiencia del cliente (CEIP) de VMware. El valor predeterminado es <code>true</code> si no se lo proporciona y no está configurado en <code>false</code> 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 <a href="http://www.vmware.com/trustvmware/ceip.html">http://www.vmware.com/trustvmware/ceip.html</a> . En cualquier momento, puede usar la herramienta de administración de celdas para unirse o abandonar el CEIP de VMware para este producto. Consulte la <a href="#">Capítulo 10 Referencia de la herramienta de administración de celdas</a> .
<code>--installer-path</code>	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 <code>vcloud.vcloud</code> .	Requiere la opción <code>--private-key-path</code> .

**Tabla 12-1. Argumentos y opciones de la utilidad de actualización de bases de datos (continuación)**

Opción	Argumento	Descripción
<code>--maintenance-cell</code>	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 actualizar las demás celdas y de haber reiniciado al menos una de ellas, esta celda se apagará y se actualizará. Requiere la opción <code>--private-key-path</code> .
<code>--multisite-user</code>	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 de usuario en la organización del sistema, se producirá un error en la actualización. Predeterminado: <code>multisite-system-account</code> .
<code>--private-key-path</code>	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 apagarán, se actualizarán y se reiniciarán de manera estable tras la actualización de la base de datos. Consulte <a href="#">Realizar una actualización orquestada de una instalación de vCloud Director</a> para obtener más información acerca de este flujo de trabajo de actualización.
<code>--unattended-upgrade</code>	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.

---

# Migrar al dispositivo de vCloud Director

# 13

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 la versión anterior existente del entorno de vCloud Director con una base de datos externa de PostgreSQL a un entorno de vCloud Director que conste de implementaciones de dispositivos de vCloud Director 10.0.

Puede migrar un entorno de vCloud Director que conste de instalaciones de vCloud Director en Linux o implementaciones de dispositivos de vCloud Director. A partir de la versión 10.0, la base de datos de Microsoft SQL ya no es compatible y solo se puede migrar un entorno de vCloud Director que use una base de datos de PostgreSQL externa.

Si el entorno de vCloud Director utiliza una base de datos de Oracle externa o una base de datos externa de Microsoft SQL, es necesario migrar a una base de datos de PostgreSQL antes de actualizar a vCloud Director 10.0. Para las rutas de acceso de actualización, consulte [Capítulo 12 Actualización de vCloud Director](#).

Este capítulo incluye los siguientes temas:

- [Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director](#)

## Migrar vCloud Director con una base de datos PostgreSQL externa al dispositivo de vCloud Director

Si el entorno actual de vCloud Director utiliza una base de datos de PostgreSQL externa, puede realizar la migración a un nuevo entorno de vCloud Director compuesto por implementaciones de dispositivos de vCloud Director. 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
- 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 de PostgreSQL externa actual tiene la versión 9.x, actualícela a la versión 10 o una posterior.
- 2 Actualice el entorno de vCloud Director actual a la versión 10.0.  
Consulte [Capítulo 12 Actualización 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`, `proxycertificates` y `truststore` que se encuentran en `/opt/vmware/vcloud-director/etc/` en `/tmp` o en cualquier ubicación que prefiera de la base de datos externa de PostgreSQL.
  - 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 10.0.

- 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, el almacén de confianza y los archivos de certificado, y copie y reemplace estos archivos de la ubicación en la base de datos de PostgreSQL externa del origen de migración a la que copió los archivos en el paso 7a.

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

- 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 Modifique la configuración del equilibrador de carga para incluir las nuevas direcciones IP del dispositivo `eth0` en los grupos del equilibrador de carga para el tráfico HTTP, HTTPS y TCP, y quite las direcciones IP de las celdas antiguas de Linux vCloud Director de esos grupos.
- 16 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 Service Provider Admin Portal mediante la dirección IP de red de `eth0` de cualquier celda del nuevo grupo de servidores, `https://eth0_IP_new_cell/provider`.
  - b Inicie sesión en Service Provider Admin Portal con las credenciales del **administrador del sistema** existentes.
  - c Compruebe que los recursos de vSphere y de nube estén disponibles en el nuevo entorno.
- 17 Después de la comprobación correcta de la migración de vCloud Director, utilice la Service Provider Admin Portal para eliminar las celdas desconectadas que pertenezcan al entorno anterior de vCloud Director.
  - a En el menú principal () , seleccione **Recursos de nube**.
  - b En el panel izquierdo, haga clic en **Celdas de nube**.
  - c Seleccione una celda inactiva y haga clic en **Eliminar del registro**.

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

# 14

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](#)

## 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 Director en 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 el menú principal () de vCloud Director Service Provider Admin Portal, seleccione **Recursos de vSphere**.
- b En el panel izquierdo, haga clic en **vCenters**.
- c Seleccione el botón de radio junto a la instancia de vCenter Server que desea deshabilitar y haga clic en **Deshabilitar**.
- d Haga clic en **Aceptar**.


### 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 el menú principal () , seleccione **Administración**.
- b En el panel izquierdo, en **Configuración**, haga clic en **Direcciones públicas**.
- c Verifique todas las direcciones públicas.

### 4 Actualice el registro de vCenter Server con vCloud Director.

- a En el menú principal () de vCloud Director Service Provider Admin Portal, seleccione **Recursos de vSphere**.
- b En el panel izquierdo, haga clic en **vCenters**.
- c Seleccione el botón de radio situado junto a la instancia de vCenter Server destino y haga clic en **Volver a conectar**.
- d Haga clic en **Aceptar**.

- 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 una puerta de enlace Edge de NSX, debe trabajar en el objeto de red de vCloud Director que admite Edge:
  - La actualización correspondiente de una puerta de enlace Edge se produce de manera automática cuando se utiliza 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.

---

**Nota** La reimplementación solo es compatible con las puertas de enlace Edge de NSX Data Center for vSphere.

---

- Al restablecer una red de vApp en el contexto de la vApp, se actualiza el dispositivo de NSX Edge asociado a esa red. Para restablecer una red de vApp desde el contexto de una vApp, desplácese hasta la pestaña **Redes** de la vApp, muestre sus detalles de red, haga clic en el botón de radio junto al nombre de la red de vApp y haga clic en **Restablecer**.

Para obtener más información sobre cómo volver a implementar puertas de enlace Edge y restablecer redes de vApp, consulte la *Guía de programación de vCloud API*.

#### Pasos siguientes

Repita este procedimiento con los demás sistemas vCenter Server registrados en su instalación de vCloud Director.



# Visualizar los registros de vCloud Director

# 15

vCloud Director proporciona información de inicio de sesión para cada celda de nube del sistema. Puede ver los registros para supervisar sus celdas y para solucionar los problemas.

Puede encontrar los registros para una celda en `/opt/vmware/vcloud-director/logs`. [Tabla 15-1. Registros de vCloud Director](#) enumera los registros disponibles.

**Tabla 15-1. Registros de vCloud Director**

Nombre de registro	Descripción
cell.log	Salida de la consola de la celda de vCloud Director.
cell-management-tool	Mensajes del registro de la herramienta de administración de celdas de la celda.
cell-runtime	Mensajes del registro del tiempo de ejecución de la celda.
cloud-proxy	Mensajes del registro del proxy de la nube de la celda.
console-proxy	Mensajes del registro del proxy de la consola remota de la celda.
server-group-communications	Comunicaciones del grupo de servidores desde la celda.
statsfeeder	Recuperación de las métricas de la máquina virtual (de vCenter Server) e información de almacenamiento, además de mensajes de error.
vcloud-container-debug.log	Mensajes del registro a nivel de depuración de la celda.
vcloud-container-info.log	Mensajes del registro de información de la celda. Este registro también muestra advertencias o errores que se encuentra la celda.
vmware-vcd-watchdog.log	Mensajes del registro de información del guardián de la celda. Registra cuándo la celda falla, se reinicia, etcétera
diagnostics.log	Registro de diagnósticos de celda. Este archivo está vacío a no ser que se haya habilitado el registro de diagnósticos en la configuración local de registro.
YYYY_MM_DD.request.log	Registros de solicitudes HTTP en el formato de registro habitual de Apache.

Puede utilizar cualquier editor/visualizador de texto o herramienta de terceros para visualizar los registros.

# Solucionar problemas del dispositivo de vCloud Director

# 16

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 `vamcli` 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 `vamcli update --check`, desplácese hasta `/opt/vmware/var/log/vami/vami.log`.
  - Si se produce un error en `vamcli 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

# 17

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.