Guía de instalación y configuración de vCloud Director

vCloud Director 8.0

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte http://www.vmware.com/es/support/pubs.

ES-001716-00

vmware®

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

http://www.vmware.com/es/support/

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Guía de instalación y actualización del VMware vCloud Director

La *Guía de instalación y actualización del VMware vCloud Director* brinda información sobre la instalación y actualización del software de VMware® vCloud Director® y la configuración del mismo a fin de que funcione con VMware vCenter™ para ofrecer servicios de VMware vCloud® habilitados para VMware.

Público objetivo

La *Guía de instalación y actualización de VMware vCloud Director* está dirigida a todos aquellos que deseen instalar o actualizar el software de VMware vCloud Director. La información contenida en este manual ha sido preparada para administradores de sistema de experiencia familiarizados con Linux, Windows, redes IP y VMware vSphere®.

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

1

VMware vCloud® combina un grupo de servidores de vCloud Director con la plataforma de vSphere. Para crear un grupo de servidores de vCloud Director, instale el software de vCloud Director en uno o más servidores, conectando los mismos a una base de datos compartida e integre el grupo de servidores de vCloud Director con vSphere.

La configuración inicial de vCloud Director, incluidos los detalles de las conexiones de red y de base de datos, se establece durante la instalación. Al actualizar una instalación existente a una nueva versión de vCloud Director, actualice el software y el esquema de datos de vCloud Director y mantenga las relaciones existentes entre los servidores, la base de datos y vSphere.

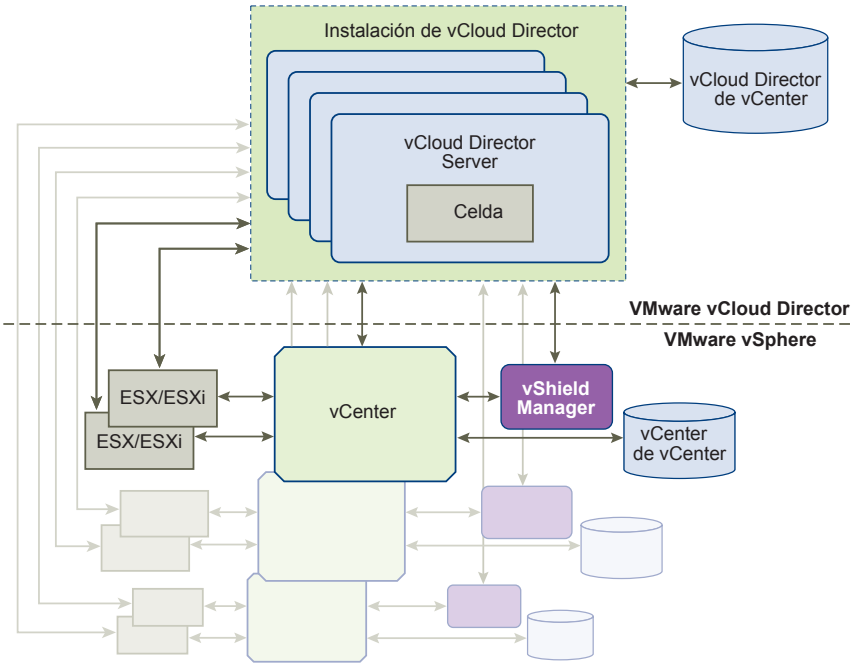
Este capítulo cubre los siguientes temas:

Arquitectura de vCloud Director

El grupo de servidores de vCloud Director consiste en uno o más vCloud Director Servers. Estos servidores comparten una base de datos común y están vinculados a un número arbitrario de sistemas vCenter Server y hosts ESXi. Los servicios de red a los sistemas vCenter Server y vCloud Director los proporciona el componente VMware vShield Manager™ de VMware vCloud® Networking and Security™ o el componente VMware NSX Manager™ de VMware NSX™ for vSphere®.

La instalación típica crea un grupo de servidores de vCloud Director que comprende varios servidores. Cada servidor del grupo ejecuta una colección de servicios denominada celda de vCloud Director. Todos los miembros del grupo comparten una sola base de datos. Cada celda del grupo se conecta con varios sistemas vCenter Server, los hosts que administran y cada vShield Manager o NSX Manager configurado para admitir cada sistema vCenter Server conectado.

Figura 1-1. Diagrama de la arquitectura de vCloud Director para una instalación que utiliza vShield Manager



El proceso de instalación y configuración de vCloud Director crea las celdas, las conecta a la base de datos compartida y establece las primeras conexiones con un sistema vCenter Server, vShield Manager o NSX Manager asociado al sistema vCenter Server y sus hosts. Un administrador del sistema puede después usar la consola web de vCloud Director para agregar sistemas vCenter Server, vShield Manager o NSX Manager asociados con el sistema vCenter Server y los hosts del sistema vCenter Server agregado al grupo de servidores de vCloud Director en cualquier momento.

Planificación de la configuración

vSphere proporciona capacidad para almacenamiento, cómputo y redes a vCloud Director. Antes de empezar la instalación, tenga en cuenta la capacidad de vSphere y vCloud Director que necesita, 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 un servidor vCloud Director (celda) por cada sistema vCenter Server que desee que esté disponible en la nube.
- Asegúrese de que todos los servidores vCloud Director satisfacen al menos los requisitos mínimos de memoria y almacenamiento que se especifican en "Requisitos de hardware y software de vCloud Director," página 9.
- Configure la base de datos de vCloud Director como se describe en "Instalación y configuración de una base de datos de vCloud Director," página 15.

Requisitos de hardware y software de vCloud Director

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 vCenter Server, a vShield Manager o NSX Manager y a uno o más hosts ESXi.

Plataformas compatibles

Existe información actual sobre las plataformas de VMware admitidas en esta versión de vCloud Director en *VMware Product Interoperability Matrixes* en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Requisitos de configuración de vSphere

Los servidores y los hosts que se pretendan utilizar con vCloud Director deben cumplir requisitos de configuración específicos.

- Las redes de vCenter que se planeen utilizar como redes externas o como grupos de redes de vCloud Director deben estar disponibles para todos los hosts en cualquier clúster destinado para que lo utilice vCloud Director. Al poner dichas redes a disposición de todos los hosts del centro de datos se simplifica la tarea de agregar nuevos vCenter Servers a vCloud Director.
- Debe utilizar switches distribuidos de vSphere para las barreras a través de hosts y para la asignación de grupos de redes.
- Los clústeres vCenter usados con vCloud Director deben configurar DRS de almacenamiento con un nivel de automatización de **Totalmente automatizado**. Esta configuración requiere que el almacenamiento compartido esté conectado a todos los hosts ESXi de un clúster de DRS. vCloud Director puede aprovechar Storage DRS, incluida la compatibilidad con aprovisionamiento rápido.
- Los vCenter Servers 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 requiere las siguientes licencias de vSphere:

- VMware DRS, licencia otorgada por vSphere Enterprise and Enterprise Plus.
- VMware Distributed Switch y dvFilter, licencia otorgada por vSphere Enterprise Plus. Esta licencia permite crear y utilizar redes aisladas de vCloud Director.

Sistemas operativos compatibles con vCloud Director Server

Tabla 1-1. Sistemas operativos compatibles con vCloud Director Server

Sistema operativo (solo de 64 bits)	Actualizaciones
CentOS 6	4
Red Hat Enterprise Linux 5	4-10
Red Hat Enterprise Linux 6	1-5

Requisitos de espacio de disco

Cada vCloud Director Server requiere aproximadamente 1450 MB de espacio libre para los archivos de instalación y de registro.

Requisitos de memoria

Cada vCloud Director Server debe aprovisionarse con al menos 4GB de memoria.

Paquetes de software de Linux

Todos los vCloud Director Servers deben incluir la instalación de varios paquetes de software de Linux. Por lo general, los paquetes se instalan de forma predeterminada con el software del sistema operativo. Si falta alguno, el instalador falla con un mensaje de diagnóstico.

Tabla 1-2. Paquetes de software requeridos

Nombre del paquete	Nombre del paquete	Nombre del paquete
alsa-lib	libICE	module-init-tools
bash	libSM	net-tools
chkconfig	libstdc	pciutils
coreutils	libX11	procps
findutils	libXau	redhat-lsb
glibc	libXdmcp	sed
grep	libXext	tar
initscripts	libXi	which
krb5-libs	libXt	
libgcc	libXtst	

NOTA: Varios procedimientos para configurar conexiones de red y crear certificados SSL requieren el uso del comando `nslookup` de Linux, que está disponible en el paquete `bind-utils` de Linux.

Bases de datos compatibles con vCloud Director

vCloud Director es compatible con bases de datos Oracle y Microsoft SQL. La información más actualizada sobre las bases de datos admitidas en esta versión de vCloud Director está disponible en *VMware Product Interoperability Matrixes* en VMware Partner Central. Inicie sesión en VMware Partner Central utilizando la información de cuenta de socio de VMware.

Para obtener las configuraciones de servidor de base de datos recomendadas, consulte "Instalación y configuración de una base de datos de vCloud Director," página 15.

Servidores LDAP compatibles

Tabla 1-3. Servidores LDAP compatibles

Plataforma	Servidor LDAP	Métodos de autenticación
Windows Server 2003	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Windows Server 2008	Active Directory	Simple
Windows 7 (2008 R2)	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Linux	OpenLDAP	Simple, Simple SSL

Compatibilidad con SO invitado

Consulte la *Guía de usuario de vCloud Director* para obtener una lista de sistemas operativos invitados compatibles.

Bases de datos admitidas para almacenar datos de métricas históricas

Puede configurar la instalación de vCloud Director para almacenar las métricas que recopila vCloud Director sobre el rendimiento y el consumo de recursos de las máquinas virtuales. Los datos de las métricas históricas se almacenan en una base de datos KairosDB respaldada por Cassandra. Consulte Capítulo 6, "Instalación y configuración de software de bases de datos opcional para almacenar y recuperar las métricas históricas del rendimiento de las máquinas virtuales," página 73 para obtener más información.

vCloud Director admite las siguientes versiones de KairosDB y Cassandra.

- KairosDB 0.9.1
- Cassandra 1.2 y 2.0

Exploradores compatibles con vCloud Director

La consola web de vCloud Director es compatible con las versiones recientes de Mozilla Firefox y Microsoft Internet Explorer.

NOTA: La consola web de vCloud Director es compatible solamente con exploradores de 32 bits. Cuando se indique que un explorador es compatible con una plataforma de 64 bits, se sobreentiende el uso del explorador de 32 bits en la plataforma de 64 bits.

Compatibilidad con exploradores en las plataformas de Linux

En estas plataformas de Linux, la consola web de vCloud Director es compatible con la versión más reciente de Mozilla Firefox y Google Chrome, y con sus versiones inmediatamente anteriores.

Tabla 1-4. Compatibilidad con exploradores y sistemas operativos en las plataformas de Linux

Plataforma	Google Chrome	Mozilla Firefox
CentOS 6.*x*	SÍ	SÍ
Red Hat Enterprise Linux 6.*x*	SÍ	SÍ
Ubuntu 12.*x*	SÍ	SÍ

Compatibilidad con exploradores en las plataformas de Windows

En las plataformas de Windows, la consola web de vCloud Director es compatible con al menos una versión de Microsoft Internet Explorer. Algunas plataformas de Windows son también compatibles con la versión más reciente de Mozilla Firefox y Google Chrome, y con sus versiones inmediatamente anteriores.

Tabla 1-5. Compatibilidad con exploradores y sistemas operativos en las plataformas de Microsoft Windows

Plataforma	Google Chrome	Mozilla Firefox	Internet Explorer 8.*x*	Internet Explorer 9.*x*	Internet Explorer 10.*x*
Windows XP Pro	SÍ	SÍ	SÍ	No	No
Windows Server 2003 Enterprise Edition	SÍ	SÍ	SÍ	No	No
Windows Server 2008	SÍ	SÍ	SÍ	SÍ	SÍ
Windows Server 2008 R2	SÍ	SÍ	SÍ	SÍ	SÍ
Windows Vista	SÍ	No	SÍ	SÍ	SÍ
Windows 7	SÍ	SÍ	SÍ	SÍ	SÍ
Windows 8	SÍ	SÍ	No	No	SÍ

Compatibilidad con exploradores en las plataformas de Macintosh

En las plataformas de Macintosh, la consola web de vCloud Director es compatible con la versión más reciente de Mozilla Firefox y Google Chrome, y con sus versiones inmediatamente anteriores.

Versiones compatibles de Adobe Flash Player

La consola web de vCloud Director requiere Adobe Flash Player 11.2 o posterior. Solo se admite la versión de 32 bits.

Versiones de Java admitidas

Los clientes de vCloud Director deben tener la actualización 10 de JRE 1.6.0 o superior instalada y activada. Solo se admite la versión de 32 bits.

Protocolos de seguridad y conjuntos de cifrado admitidos

vCloud Director requiere conexiones de los clientes para que sea seguro. SSL versión 3 ha demostrado tener graves vulnerabilidades de seguridad por lo que ya no es uno de los conjuntos de protocolos predeterminados que el servidor se ofrece a utilizar al realizar una conexión del cliente. Se admiten los siguientes protocolos de seguridad:

- TLS versión 1.0
- TLS versión 1.1
- TLS versión 1.2

Puede utilizar `cell-management-tool` para volver a configurar el conjunto de protocolos predeterminados. Consulte "Administrar la lista de protocolos SSL permitidos," página 68.

Los conjuntos de cifrado compatibles incluyen los de firma RSA, DSS o de curva elíptica, y los cifrados DES3, AES-128 o AES-256. Puede utilizar `cell-management-tool` para volver a configurar el conjunto de cifrados SSL admitidos. Véase "Administrar la lista de cifrados SSL permitidos," página 66

Resumen de los requisitos de configuración de red de 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 vCloud Director, el servidor de base de datos, los servidores vCenter y los componentes asociados de vCloud Networking and Security o NSX for vSphere deben satisfacer varios requisitos:

direcciones IP

Cada vCloud Director Server requiere dos direcciones IP para que pueda admitir dos conexiones SSL distintas. Una conexión es para el servicio HTTP. La otra es para el servicio de proxy de consola. Puede utilizar alias de IP o varias interfaces de red para crear dichas direcciones. No puede utilizar el comando `ip addr add` de Linux para crear la segunda dirección.

Dirección del proxy de consola

La dirección IP configurada como dirección 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.

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 nombre 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
```

Almacenamiento de 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. Cuando NFS se utiliza como almacenamiento de servidor de transferencia, deben establecerse algunos valores de configuración de modo que cada celda de vCloud Director en el grupo de servidores de vCloud Director pueda montar y utilizar el almacenamiento de servidor de transferencia con NFS. Consulte http://kb.vmware.com/kb/2086127 para obtener más detalles. Todos los

miembros del grupo de servidores deben montar 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:

- Las transferencias (cargas y descargas) ocupan este almacenamiento mientras la transferencia está en curso y se eliminan cuando la transferencia finaliza. 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.
- Los elementos de catálogo de los catálogos que se publican externamente y habilitan el almacenamiento en caché del contenido publicado ocupan este almacenamiento mientras existen. (Los elementos de los catálogos que se publican externamente pero no habilitan el almacenamiento en caché no ocupan este almacenamiento.) Si permite a las organizaciones de su nube crear catálogos que se publicarán externamente, la opción más segura es asumir que cientos o incluso miles de elementos de catálogo necesitarán espacio en este volumen y que cada elemento de catálogo tendrá el tamaño de una máquina virtual en formato OVF comprimido.

NOTA: Si es posible, el volumen que utilice para el almacenamiento del servidor de transferencia debe ser un volumen cuya capacidad se pueda ampliar fácilmente.

Recomendaciones para la 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 todo el resto del tráfico entrante proveniente de redes públicas.

Tabla 1-6. 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	ActiveMQ
61616	TCP	ActiveMQ

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

Tabla 1-7. 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	vCenter, vShield Manager, NSX Manager y conexiones ESX
514	UDP	Opcional. Permite el uso de syslog.
902	TCP	Conexiones de vCenter y de ESX.
903	TCP	Conexiones de vCenter y de ESX.
920	TCP, UDP	rpc.statd de NFS utilizado por el servicio de transferencia.
1433	TCP	Puerto de base de datos de Microsoft SQL Server predeterminado.
1521	TCP	Puerto de base de datos Oracle predeterminado.
5672	TCP, UDP	Opcional. Mensajes de AMQP para las extensiones de tareas.
61611	TCP	ActiveMQ
61616	TCP	ActiveMQ

- Tráfico de ruta entre los vCloud Director Servers y el servidor de base de datos de vCloud Director a través de una red privada dedicada, si es posible.
- 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 nivel 2.

Instalación y configuración de una base de datos de vCloud Director

Las celdas de vCloud Director utilizan una base de datos para almacenar la información compartida. Dicha base de datos debe existir antes para poder completar la instalación y configuración del software de vCloud Director.

NOTA: Independientemente del software de base de datos que elija, debe crear un esquema de base de datos separado y dedicado para que lo utilice vCloud Director. vCloud Director no puede compartir un esquema de base de datos con ningún otro producto de VMware.

Configuración de una base de datos de Oracle

Las bases de datos de Oracle tienen requisitos de configuración específicos cuando se utilizan con vCloud Director. Instale y configure una instancia de base de datos y cree la cuenta de usuario de la base de datos de vCloud Director antes de instalar vCloud Director.

Procedimiento

1 Configure el servidor de base de datos.

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

2 Cree la instancia de la base de datos.

Utilice un comando con el siguiente formato para crear un único espacio de tabla CLOUD_DATA:

```
Create Tablespace CLOUD_DATA datafile '$ORACLE_HOME/oradata/cloud_data01.dbf' size 1500M
autoextend on;
```

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

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

```
Create user $vcloud identified by $vcloudpass default tablespace CLOUD_DATA;
```

NOTA: Al crear la cuenta de usuario de la base de datos de vCloud Director, debe especificar CLOUD_DATA como el espacio de tabla predeterminado.

4 Configure los parámetros de conexión, proceso y transacción de la base de datos.

Debe configurarse la base de datos de modo que permita al menos 75 conexiones por cada celda de vCloud Director, además de alrededor de 50 para el propio uso de Oracle. Puede obtener valores para los demás parámetros de configuración en función de la cantidad de conexiones, donde *C* representa el número de celdas del clúster de vCloud Director.

Parámetro de configuración de Oracle	Valor de las celdas de *C*
CONNECTIONS	75*C+50
PROCESSES	= CONNECTIONS
SESSIONS	= PROCESSES*1.1+5
TRANSACTIONS	= SESSIONS*1.1
OPEN_CURSORS	= SESSIONS

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

No utilice la cuenta del sistema de Oracle como la cuenta de usuario de la base de datos de vCloud Director. Debe crear una cuenta de usuario dedicada para este fin. Conceda los siguientes privilegios del sistema a la cuenta:

- CONNECT
- RESOURCE
- CREATE TRIGGER
- CREATE TYPE
- CREATE VIEW
- CREATE MATERIALIZED VIEW

- CREATE PROCEDURE
- CREATE SEQUENCE

6 Anote el nombre del servicio de la base de datos para que pueda utilizarlo al configurar las conexiones de red y de base de datos.

Para obtener el nombre del servicio de la base de datos, abra el archivo `$ORACLE_HOME/network/admin/tnsnames.ora` en el servidor de la base de datos y busque una entrada similar a:

```
(SERVICE_NAME = orcl.example.com)
```

Configuración de una base de datos de Microsoft SQL Server

Las bases de datos de SQL Server tienen requisitos de configuración específicos cuando se utilizan con vCloud Director. Instale y configure una instancia de base de datos y cree la cuenta de usuario de la base de datos de vCloud Director antes de instalar vCloud Director.

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

Prerequisitos

- Debe estar familiarizado con el funcionamiento, la creación de scripts y los comandos de Microsoft SQL Server.
- Para configurar Microsoft SQL Server, inicie sesión en el equipo host de SQL Server con las credenciales de administrador. Configure SQL Server para ejecutar la identidad LOCAL_SYSTEM, o cualquier otra identidad con privilegios para ejecutar un servicio de Windows.

Procedimiento

1 Configure el servidor de base de datos.

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

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

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

3 Cree la instancia de la base de datos.

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

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

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

4 Establezca el nivel de aislamiento de la transacción.

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

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

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

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

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

```
USE [vcloud]
GO
CREATE LOGIN [vcloud] WITH PASSWORD = 'vcloudpass', DEFAULT_DATABASE =[vcloud],
   DEFAULT_LANGUAGE =[us_english], CHECK_POLICY=OFF
GO
CREATE USER [vcloud] for LOGIN [vcloud]
GO
```

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

El siguiente script asigna la función `db_owner` al usuario de la base de datos creado en Step 5.

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

Creación de certificados SSL

vCloud Director usa SSL para proteger la comunicación entre clientes y servidores. Antes de instalar y configurar un grupo de servidores de vCloud Director, debe crear dos certificados para cada miembro del grupo e importar los certificados en los almacenes de claves del host.

Cada servidor de vCloud Director requiere dos direcciones IP para que pueda admitir dos extremos SSL distintos. Cada extremo requiere su propio certificado SSL. Los certificados para ambos extremos deben incluir un nombre distintivo X.500. Muchas autoridades de certificación recomiendan incluir una extensión con nombre de sujeto alternativo X.509 en los certificados que otorgan. vCloud Director no requiere que los certificados incluyan un nombre de sujeto alternativo.

Procedimiento

1 Enumere las direcciones IP del servidor.

Utilice un comando como `ifconfig` para detectar las direcciones IP del servidor.

2 Para cada dirección IP, ejecute el comando siguiente a fin de recuperar el nombre de dominio totalmente cualificado al cual esté enlazada la dirección IP.

```
nslookup ip-address
```

3 Anote cada dirección IP, el nombre del dominio totalmente cualificado asociado a ella y si vCloud Director debería utilizar la dirección para el servicio HTTP o para el servicio de proxy de consola.

   Necesitará los nombres de dominio totalmente cualificados cuando cree los certificados y las direcciones IP cuando configure las conexiones de red y de base de datos. Si hay otros nombres de dominio completos que pueden conectarse a la dirección IP, anótelos también, ya que tendrá que proporcionarlos si quiere que el certificado incluya un nombre de sujeto alternativo.

4 Cree los certificados.

   Puede utilizar certificados firmados por una autoridad de certificación de confianza o bien, certificados de firma automática.

   NOTA: Los certificados firmados ofrecen el nivel más alto de confianza.

Creación e importación de certificados SSL firmados

Los certificados firmados brindan el más alto nivel de confianza en las comunicaciones de SSL.

Cada servidor vCloud Director requiere dos certificados SSL, uno para el servicio HTTP y otro para el servicio de proxy de consola en un archivo de almacén de claves Java. Puede utilizar certificados firmados por una autoridad de certificación de confianza o bien, certificados de firma automática. Los certificados firmados ofrecen el nivel más alto de confianza.

IMPORTANTE: En estos ejemplos de especifica un tamaño de clave de 2.048 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 1.024 bits ya no se admiten según la publicación especial NIST 800-131A.

Para crear e importar certificados de firma automática, consulte "Creación de certificados SSL de firma automática," página 22.

Prerequisitos

- Genere una lista de nombres de dominio completos y sus direcciones IP asociadas en este servidor.
- Elija una dirección para usar con el servicio HTTP y una dirección para usar con el servicio de proxy de consola. Consulte "Creación de certificados SSL," página 18.
- Verifique que tiene acceso al equipo que tiene una versión 7 de Java Runtime Environment, para que pueda crear el certificado utilizando el comando `keytool`. 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 que tenga instalada la versión 7 de Java Runtime Environment. Los certificados que hayan sido creados con el comando `keytool` desde cualquier otra fuente no se admiten en vCloud Director. El efectuar la creación e importación de los certificados antes de instalar y configurar el software de vCloud Director simplifica el proceso de instalación y configuración. Estos ejemplos de línea de comandos dan por sentado que `keytool` se encuentra en la ruta del usuario. La contraseña del almacén de claves se representa en estos ejemplos como *passwd*.
- Los certificados para ambos extremos deben incluir un nombre distintivo X.500. Muchas autoridades de certificación recomiendan incluir una extensión con nombre de sujeto alternativo X.509 en los certificados que otorgan. vCloud Director no requiere que los certificados incluyan un nombre de sujeto alternativo. Familiarícese con el comando `keytool`, incluidas sus opciones `-dname` y `-ext`.

- Recopile la información requerida para el argumento en la opción `–dname` de keytool.

Tabla 1-8. Información requerida por la opción `–dname` de keytool

Subparte del nombre distintivo X.500	palabra clave keytool	Descripción	Ejemplo
commonName	CN	Nombre de dominio completo asociado con la dirección IP de este extremo.	CN=vcd1.example.com
organizationalUnit	OU	Nombre de una unidad organizativa, como un departamento o división dentro de la organización, con la que se asocia este certificado	OU=Engineering
organizationName	O	Nombre de la organización con la que se asocia este certificado	O=Example Corporation
localityName	L	Nombre de la ciudad en la que se ubica la organización.	L=Palo Alto
stateName	S	Nombre del país o región en la que se ubica la organización.	S=California
país	C	Nombre del país en el que se ubica la organización.	C=US

Procedimiento

1 Cree un certificado que no sea de confianza para el servicio HTTP.

Este comando de ejemplo crea un certificado que no es de confianza en un archivo de almacén de claves denominado `certificates.ks`. Las opciones `keytool` se han colocado en líneas separadas para clarificar. La información de nombre distintivo X.500 ofrecida en el argumento a la opción `–dname` emplea los valores mostrados en los requisitos previos. Los valores DNS e IP mostrados en el argumento para la opción`–ext` son típicos. Asegúrese de incluir todos los nombres DNS en los que se puede alcanzar este extremo, incluido el que especificó para el valor `commonName` (CN) en el argumento de opción `–dname`. También puede incluir direcciones IP, como se muestra a continuación.

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

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.

2 Cree un certificado que no sea de confianza para el servicio proxy de consola.

Este comando agrega un certificado que no es de confianza al archivo de almacén de datos creado en Step 1. Las opciones `keytool` se han colocado en líneas separadas para clarificar. La información de nombre distintivo X.500 ofrecida en el argumento a la opción `–dname` emplea los valores mostrados en los requisitos previos. Los valores DNS e IP mostrados en el argumento a la opción `–ext` son típicos. Asegúrese de incluir todos los nombres DNS en los que se puede alcanzar este extremo, incluido el que especificó para el valor `commonName` (CN) en el argumento de opción `–dname`. También puede incluir direcciones IP, como se muestra a continuación.

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 Cree una solicitud de firma de certificado para el servicio HTTP.

Este comando crea una solicitud de firma de certificado en el archivo `http.csr`.

```
keytool –keystore certificates.ks –storetype JCEKS –storepass passwd –certreq –alias http –
file http.csr
```

4 Cree una solicitud de firma de certificado para el servicio de proxy de consola.

Este comando crea una solicitud de firma de certificado en el archivo `consoleproxy.csr`.

```
keytool –keystore certificates.ks –storetype JCEKS –storepass passwd –certreq –alias
consoleproxy –file consoleproxy.csr
```

5 Envíe las solicitudes de firma de certificado a la autoridad de certificación.

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

6 Cuando reciba los certificados firmados, impórtelos en el archivo de almacén de claves.

a Importe el certificado raíz de la autoridad de certificación en el archivo de almacén de claves.

Este comando importa el certificado raíz del archivo `root.cer` al archivo de almacén de claves `certificates.ks`.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias root
–file root.cer
```

b (Opcional) Si recibió certificados intermedios, impórtelos en el archivo de almacén de claves.

Este comando importa los certificados intermedios del archivo `intermediate.cer` al archivo de almacén de claves `certificates.ks`.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –import –alias
intermediate –file intermediate.cer
```

c Importe el certificado del servicio HTTP.

Este comando importa el certificado del archivo `http.cer` al archivo de almacén de claves `certificates.ks`.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias http
-file http.cer
```

d Importe el certificado del servicio de proxy de consola.

Este comando importa el certificado del archivo `consoleproxy.cer` al archivo de almacén de claves `certificates.ks`.

```
keytool -storetype JCEKS -storepass passwd -keystore certificates.ks -import -alias
consoleproxy -file consoleproxy.cer
```

7 Para verificar que se hayan importado todos los certificados, vea el contenido del archivo de almacén de claves.

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

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

Qué hacer a continuación

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 almacén de claves cuando ejecute el script de configuración. Consulte "Configuración de conexiones de red y de base de datos," página 32.

Creación de certificados SSL de firma automática

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 vCloud Director requiere dos certificados SSL, uno para el servicio HTTP y otro para el servicio de proxy de consola en un archivo de almacén de claves Java. Puede utilizar certificados firmados por una autoridad de certificación de confianza o bien, certificados de firma automática. Los certificados firmados ofrecen el nivel más alto de confianza.

IMPORTANTE: En estos ejemplos de especifica un tamaño de clave de 2.048 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 1.024 bits ya no se admiten según la publicación especial NIST 800-131A.

Para crear e importar certificados firmados, consulte "Creación e importación de certificados SSL firmados," página 19.

Prerequisitos

- Genere una lista de nombres de dominio completos y sus direcciones IP asociadas en este servidor.
- Elija una dirección para usar con el servicio HTTP y una dirección para usar con el servicio de proxy de consola. Consulte "Creación de certificados SSL," página 18.
- Verifique que tiene acceso al equipo que tiene una versión 7 de Java Runtime Environment, para que pueda crear el certificado utilizando el comando `keytool`. 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 que tenga instalada la versión 7 de Java Runtime Environment. Los certificados que hayan sido creados con el comando `keytool` desde cualquier otra fuente no se admiten en vCloud Director. El efectuar la creación e importación de los certificados antes de instalar y configurar el software de vCloud Director simplifica el proceso de instalación y configuración. Estos ejemplos de línea de comandos dan por sentado que `keytool` se encuentra en la ruta del usuario. La contraseña del almacén de claves se representa en estos ejemplos como *passwd*.

- Los certificados para ambos extremos deben incluir un nombre distintivo X.500. Muchas autoridades de certificación recomiendan incluir una extensión con nombre de sujeto alternativo X.509 en los certificados que otorgan. vCloud Director no requiere que los certificados incluyan un nombre de sujeto alternativo. Familiarícese con el comando `keytool`, incluidas sus opciones `–dname` y `–ext`.
- Recopile la información requerida para el argumento en la opción `–dname` de keytool.

Tabla 1-9. Información requerida por la opción `–dname` de keytool

Subparte del nombre distintivo X.500	palabra clave keytool	Descripción	Ejemplo
commonName	CN	Nombre de dominio completo asociado con la dirección IP de este extremo.	CN=vcd1.example.com
organizationalUnit	OU	Nombre de una unidad organizativa, como un departamento o división dentro de la organización, con la que se asocia este certificado	OU=Engineering
organizationName	O	Nombre de la organización con la que se asocia este certificado	O=Example Corporation
localityName	L	Nombre de la ciudad en la que se ubica la organización.	L=Palo Alto
stateName	S	Nombre del país o región en la que se ubica la organización.	S=California
país	C	Nombre del país en el que se ubica la organización.	C=US

Procedimiento

1 Cree un certificado que no sea de confianza para el servicio HTTP.

Este comando de ejemplo crea un certificado que no es de confianza en un archivo de almacén de claves denominado `certificates.ks`. Las opciones `keytool` se han colocado en líneas separadas para clarificar. La información de nombre distintivo X.500 ofrecida en el argumento a la opción `–dname` emplea los valores mostrados en los requisitos previos. Los valores DNS e IP mostrados en el argumento para la opción `–ext` son típicos. Asegúrese de incluir todos los nombres DNS en los que se puede alcanzar este extremo, incluido el que especificó para el valor `commonName` (CN) en el argumento de opción `–dname`. También puede incluir direcciones IP, como se muestra a continuación.

```
keytool
   –keystore certificates.ks
   –alias http
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd1.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd1.example.com,dns:vcd1,ip:10.100.101.9"
```

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.

2 Cree un certificado que no sea de confianza para el servicio proxy de consola.

Este comando agrega un certificado que no es de confianza al archivo de almacén de datos creado en Step 1. Las opciones `keytool` se han colocado en líneas separadas para clarificar. La información de nombre distintivo X.500 ofrecida en el argumento a la opción `–dname` emplea los valores mostrados en los requisitos previos. Los valores DNS e IP mostrados en el argumento a la opción `–ext` son típicos. Asegúrese de incluir todos los nombres DNS en los que se puede alcanzar este extremo, incluido el que especificó para el valor `commonName` (CN) en el argumento de opción `–dname`. También puede incluir direcciones IP, como se muestra a continuación.

```
keytool
   –keystore certificates.ks
   –alias consoleproxy
   –storepass passwd
   –keypass passwd
   –storetype JCEKS
   –genkeypair
   –keyalg RSA
   –keysize 2048
   –validity 365
   –dname "CN=vcd2.example.com, OU=Engineering, O=Example Corp, L=Palo Alto S=California
C=US"
   –ext "san=dns:vcd2.example.com,dns:vcd2,ip:10.100.101.10"
```

3 Para verificar que se hayan importado todos los certificados, vea el contenido del archivo de almacén de claves.

```
keytool –storetype JCEKS –storepass passwd –keystore certificates.ks –list
```

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

Qué hacer a continuación

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 almacén de claves cuando ejecute el script de configuración. Consulte "Configuración de conexiones de red y de base de datos," página 32.

Instalación y configuración de vShield Manager para una nueva instalación de vCloud Director

vCloud Director está supeditado a disponer de vShield Manager o NSX Manager para ofrecer servicios de red a la nube. Antes de llevar a cabo una instalación nueva de vCloud Director, debe instalar y configurar vShield Manager o NSX Manager y asociar una instancia única de vShield Manager o NSX Manager con cada vCenter Server que piensa incluir en la instalación de vCloud Director.

vShield Manager se incluye en la descarga de VMware vCloud Networking and Security. La información más actualizada sobre las versiones de vShield Manager compatibles con vCloud Director está disponible en *VMware Product Interoperability Matrixes* en VMware Partner Central. Inicie sesión en VMware Partner Central utilizando la información de cuenta de socio de VMware. Para obtener más información sobre los requisitos de red, consulte "Requisitos de hardware y software de vCloud Director," página 9.

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 3, "Actualización de vCloud Director," página 41.

Prerequisitos

- Verifique que cada sistema vCenter Server satisface los requisitos previos para la instalación de vShield Manager.
- Lleve a cabo la tarea de instalación del dispositivo virtual vShield Manager descrito en la *Guía de instalación y actualización de vShield*.

Procedimiento

1 Inicie sesión en el dispositivo virtual vShield Manager que instaló y confirme la configuración que especificó durante la instalación.

2 Asocie el dispositivo virtual vShield Manager que instaló con el sistema vCenter Server que piensa agregar a vCloud Director en la instalación planificada de vCloud Director.

Qué hacer a continuación

Configure la compatibilidad VXLAN en el vShield Manager asociado. 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 con vShield 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 la *Guía de administración de vShield*.

Instalación y configuración de NSX Manager para una nueva instalación de vCloud Director

vCloud Director está supeditado a disponer de vShield Manager o NSX Manager para ofrecer servicios de red a la nube. Antes de llevar a cabo una instalación nueva de vCloud Director, debe instalar y configurar vShield Manager o NSX Manager y asociar una instancia única de vShield Manager o NSX Manager con cada vCenter Server que piensa incluir en la instalación de vCloud Director.

NSX se incluye en la descarga de VMware NSX for vSphere. La información más actualizada sobre las versiones de NSX Manager compatibles con vCloud Director está disponible en *VMware Product Interoperability Matrixes* en VMware Partner Central. Inicie sesión en VMware Partner Central utilizando la información de cuenta de socio de VMware. Para obtener más información sobre los requisitos de red, consulte "Requisitos de hardware y software de vCloud Director," página 9.

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 3, "Actualización de vCloud Director," página 41.

Prerequisitos

- Verifique que cada sistema vCenter Server satisface los requisitos previos para la instalación de NSX Manager.
- Lleve a cabo la tarea de instalación del dispositivo virtual NSX Manager descrito en la *Guía de instalación y actualización de NSX*.

Procedimiento

1 Inicie sesión en el dispositivo virtual NSX Manager que instaló y confirme la configuración que especificó durante la instalación.

2 Asocie el dispositivo virtual NSX Manager que instaló con el sistema vCenter Server que piensa agregar a vCloud Director en la instalación planificada de vCloud Director.

Qué hacer a continuación

Configure la compatibilidad VXLAN en el dispositivo NSX Manager asociado. 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 la *Guía de administración de NSX*.

Instalación y configuración de un broker AMQP

El protocolo de cola de mensajes avanzado (AMQP, Advanced Message Queuing Protocol) es un estándar abierto para poner mensajes en cola que admite mensajes flexibles en sistemas empresariales. vCloud Director incluye un servicio AMQP que se puede configurar para que funcione con un broker AMQP, como RabbitMQ, que ofrece a los operadores de nubes una secuencia de notificaciones de los eventos en la nube. Si desea utilizar este servicio, instale y configure un broker AMQP.

Aunque el uso de un broker AMQP con vCloud Director es opcional, varias integraciones utilizan AMQP para comunicarse con vCloud Director. Consulte en los documentos relativos a la instalación y configuración los detalles sobre las integraciones que haya planificado.

Procedimiento

1 Descargue el servidor de RabbitMQ de http://info.vmware.com/content/12834_rabbitmq.

2 Siga las instrucciones de instalación de RabbitMQ para instalar RabbitMQ en un host apropiado.

  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 especificar al configurar vCloud Director para 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 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 "/".

Qué hacer a continuación

El servicio AMQP de vCloud Director envía mensajes sin cifrar AMQP de manera predeterminada. Si lo configura para cifrar estos mensajes mediante SSL, verifica el certificado del broker utilizando el almacén de confianza JCEKS predeterminado del entorno Java Runtime Environment del servidor de vCloud Director. Java Runtime Environment se encuentra generalmente en el directorio `$JRE_HOME/lib/security/cacerts`.

Para utilizar SSL con el servicio AMQP de vCloud Director, seleccione **Utilizar SSL** en la sección Configuración de broker AMQP de la página Extensibilidad de la consola web de vCloud Director y proporcione:

- un nombre de ruta de certificado SSL o
- un nombre de ruta y contraseña de almacén de confianza de JCEKS

Si no necesita validar el certificado de broker de AMQP, puede seleccionar **Aceptar todos los certificados**.

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.

Creación de un grupo de servidores de vCloud Director 2

Un grupo de servidores de vCloud Director consta de uno o varios servidores de vCloud Director que comparten una base de datos común y otros detalles de configuración. Para crear un grupo de servidores, instale y configure el software de vCloud Director en el primer miembro del grupo. La instalación y configuración del primer miembro del grupo crea un archivo de respuesta que debe utilizar para configurar miembros adicionales del grupo.

Requisitos previos para la creación de un grupo de servidores de vCloud Director

IMPORTANTE: Este procedimiento es solo para instalaciones nuevas. Si va a actualizar una instalación existente de vCloud Director, consulte Capítulo 3, "Actualización de vCloud Director," página 41.

Antes de comenzar la instalación y configuración de vCloud Director, realice todas las tareas siguientes.

1. Verifique que esté en funcionamiento un sistema vCenter Server compatible y que se haya configurado para utilizarse con vCloud Director. Para averiguar las versiones compatibles y los requisitos de configuración, consulte "Plataformas compatibles," página 9.
2. Verifique que está en funcionamiento un sistema vShield Manager o NSX Manager compatible, asociado con el sistema vCenter Server y que se haya configurado para utilizarse con vCloud Director. Para averiguar las versiones compatibles, consulte "Plataformas compatibles," página 9. Para obtener los detalles de instalación y configuración, consulte "Instalación y configuración de vShield Manager para una nueva instalación de vCloud Director," página 24 y "Instalación y configuración de NSX Manager para una nueva instalación de vCloud Director," página 25.
3. Verifique que tiene al menos una plataforma de servidores compatible para ejecutar el software vCloud Director y que dicha plataforma está configurada con la cantidad apropiada de memoria y almacenaje. Para averiguar las plataformas compatibles y los requisitos de configuración, consulte "Sistemas operativos compatibles con vCloud Director Server," página 10.
   - Cada miembro del grupo de servidores requiere dos direcciones IP: una que pueda admitir una conexión SSL para el servicio HTTP y otra para el servicio proxy de consola.
   - Cada servidor debe tener un certificado SSL por cada dirección IP. Todos los usuarios deben poder leer todos los directorios en el nombre de ruta a los certificados SSL. Consulte "Creación de certificados SSL," página 18.
   - Para el servicio de transferencias, todos los servidores deben montar un NFS o cualquier otro volumen de almacenamiento compartido en `/opt/vmware/vcloud-director/data/transfer`. Este volumen debe estar accesible para todos los miembros del grupo de servidores. Consulte "Resumen de los requisitos de configuración de red de vCloud Director," página 13.
   - Cada servidor debe tener acceso a un paquete de implementación de Microsoft Sysprep. Consulte "Instalar archivos de Microsoft Sysprep en los servidores," página 37.

4 Verifique que se ha creado una base de datos de vCloud Director y que la misma sea accesible para todos los servidores del grupo. Para obtener una lista del software de base de datos compatible, consulte "Bases de datos compatibles con vCloud Director," página 10.

   - Verifique que ha creado una cuenta para el usuario de a base de datos de vCloud Director y que la cuenta dispone de todos los privilegios de base de datos necesarios. Consulte "Instalación y configuración de una base de datos de vCloud Director," página 15.
   - Verifique que el servicio de la base de datos se inicie cuando el servidor de base de datos se rearranque.

5 Verifique que todos los servidores vCloud Director, el servidor de base de datos, todos los sistemas vCenter Server y los componentes vShield Manager o NSX Manager asociados a esos sistemas vCenter Server pueden resolver los nombres de cada uno de ellos entre sí como se describe en "Resumen de los requisitos de configuración de red de vCloud Director," página 13.

6 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 "Resumen de los requisitos de configuración de red de vCloud Director," página 13.

7 Si planea importar usuarios o grupos a partir de un servicio LDAP, verifique que el servicio sea accesible para cada vCloud Director Server.

8 Abra los puertos de firewall, tal como se ilustra en "Recomendaciones para la seguridad de red," página 14. El puerto 443 debe estar abierto entre vCloud Director y los sistemas vCenter Server.

Este capítulo cubre los siguientes temas:

Instalación y configuración del software de vCloud Director en el primer miembro de un grupo de servidores

Todos los miembros de vCloud Director compartirán la conexión de base de datos y otros detalles de configuración que especifique al instalar y configurar el primer miembro del grupo. Estos detalles se registran en el archivo de respuesta, que deberá utilizar cuando añada miembros al grupo.

El software de vCloud Director se distribuye como un archivo ejecutable de Linux firmado digitalmente denominado `vmware-vcloud-director-8.0.0-`*nnnnnn*`.bin`, donde *nnnnnn* representa el número de compilación.

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. Después de que se instale el software en el servidor de destino, debe ejecutar un script que configure las conexiones de red y de base de datos del servidor. Este script crea un archivo de respuesta que deberá utilizar al configurar los miembros adicionales de este grupo de servidores.

Prerequisitos

- Compruebe que el servidor de destino y la red que lo conecta cumplan los requisitos especificados en"Resumen de los requisitos de configuración de red de vCloud Director," página 13.

- Verifique que dispone de credenciales de superusuario en el servidor de destino.
- Compruebe que el servidor de destino monta el volumen de almacenamiento del servicio de transferencia compartido en `/opt/vmware/vcloud-director/data/transfer`.
- Para 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," página 27.

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 CD o en otro medio, copie el archivo de instalación en una ubicación que sea accesible para todos los servidores de destino.

3 Compruebe que la suma de comprobación de la descarga coincide 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 coincide con el que aparece 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
checksum-value installation-file
```

Compare el valor *checksum-value* que produce este comando con la suma de comprobación MD5 copiada de la página descargada.

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 en una ventana de consola, shell o terminal.

Para ejecutar el archivo de instalación, especifique su 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.

El instalador imprime la siguiente advertencia si no ha instalado la clave pública de VMware en el servidor de destino.

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

Cuando se ejecuta el instalador, lleva a cabo estas acciones.

a Comprueba que el host cumple todos los requisitos

b Verifica la firma digital del archivo de instalación

c Crea el usuario y grupo `vcloud`

d Desempaqueta el paquete RPM de vCloud Director

e Instala el software

Después de instalar el software, el instalador le indicará que ejecute el script de configuración, que configura las conexiones de red y base de datos del servidor.

Qué hacer a continuación

Decida si se ejecutará el script de configuración.

- Si ha completado los requisitos previos incluidos en "Requisitos previos para la creación de un grupo de servidores de vCloud Director," página 29, podrá ejecutar el script de configuración ahora. Escriba **y** y pulse Entrar.
- Si no está preparado para ejecutar ahora el script de configuración, escriba **n** y pulse Entrar para salir del shell.

Para obtener más información en cuanto a la ejecución del script, consulte "Configuración de conexiones de red y de base de datos," página 32.

Configuración de conexiones de red y de base de datos

Después de instalar el software de vCloud Director en el servidor, el instalador le indica que ejecute un script que configura las conexiones de red y de base de datos del servidor.

Debe instalar el software de vCloud Director en el servidor para poder ejecutar el script de configuración. El instalador le indica que ejecute el script después de que se complete la instalación, pero puede optar por ejecutarlo posteriormente.

Para ejecutar el script después de que se instale el software de vCloud Director, inicie sesión como usuario raíz, abra una ventana de consola, shell o terminal y escriba:

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

El script de configuración crea conexiones de red y de base de datos para un solo vCloud Director Server. El script también crea un archivo de respuesta que conserva la información de conexión de la base de datos, la cual se puede utilizar en instalaciones de servidor subsiguientes.

NOTA: Después de ejecutar el script de configuración para configurar el primer miembro del grupo de servidores, debe utilizar la opción `-r` y especificar el nombre de ruta del archivo de respuesta cuando configure miembros adicionales del grupo. Consulte "Protección y reutilización del archivo de respuesta," página 35.

Prerequisitos

- Verifique que una base de datos de un tipo compatible esté accesible desde el vCloud Director Server. Consulte "Instalación y configuración de una base de datos de vCloud Director," página 15 y "Requisitos de hardware y software de vCloud Director," página 9.
- Debe tener la siguiente información disponible:
  - Ubicación y contraseña del archivo de almacén de claves que incluya los certificados SSL de este servidor. Consulte "Creación e importación de certificados SSL firmados," página 19. El script de configuración no se ejecuta con una identidad privilegiada, por lo que todos los usuarios deben poder leer el archivo del almacén de claves y el directorio en el que está almacenado.
  - Contraseña de cada certificado SSL.
  - Nombre de host o dirección IP del servidor de base de datos.
  - Nombre y puerto de conexión de la base de datos.
  - Credenciales de usuario de la base de datos (nombre de usuario y contraseña). El usuario debe contar con privilegios de base de datos específicos. Consulte "Instalación y configuración de una base de datos de vCloud Director," página 15.

Procedimiento

1 Especifique las direcciones IP que se utilizarán con los servicios de HTTP y de proxy de consola en este host.

Cada miembro de un grupo de servidores requiere dos direcciones IP para poder admitir dos conexiones SSL diferentes: una para el servicio HTTP y otra para el servicio de proxy de consola. Para comenzar el proceso de configuración, elija las direcciones IP detectadas por el script que deben utilizarse con cada servicio.

```
Please indicate which IP address available on this machine should be used for the HTTP
service and which IP address should be used for the remote console proxy. The HTTP service
IP address is used for accessing the user interface and the REST API. The remote console
proxy IP address is used for all remote console (VMRC) connections and traffic. Please enter
your choice for the HTTP service IP address: 1: 10.17.118.158 2: 10.17.118.159 Choice
[default=1]:2
Please enter your choice for the remote console proxy IP address 1: 10.17.118.158 Choice
[default=1]:
```

2 Especifique la ruta completa al archivo del almacén de claves de Java.

```
Please enter the path to the Java keystore containing your SSL certificates and private
keys:/opt/keystore/certificates.ks
```

3 Especifique las contraseñas del almacén de claves y del certificado.

```
Please enter the password for the keystore: Please enter the private key password for the
'http' SSL certificate: Please enter the private key password for the 'consoleproxy' SSL
certificate:
```

4 Configure las opciones de administración de 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` además de a la base de datos de vCloud Director.

Opción	Acción
Para registrar los mensajes de auditoría tanto en `syslog` como en la base de datos de vCloud Director.	Especifique el nombre del host o la dirección IP de `syslog`.
Para registrar los mensajes de auditoría solamente en la base de datos de vCloud Director	Pulse Entrar.

```
If you would like to enable remote audit logging to a syslog host please enter the hostname
or IP address of the syslog server. Audit logs are stored by vCloud Director for 90 days.
Exporting logs via syslog will enable you to preserve them for as long as necessary. Syslog
host name or IP address [press Enter to skip]:10.150.10.10
```

5 Especifique el puerto en el cual el proceso `syslog` supervisa el servidor especificado.

El puerto predeterminado es 514.

```
What UDP port is the remote syslog server listening on? The standard syslog port is 514.
[default=514]: Using default value "514" for syslog port.
```

6 Especifique el tipo de base de datos o pulse Entrar para aceptar el valor predeterminado.

```
The following database types are supported: 1. Oracle 2. Microsoft SQL Server Enter the
database type [default=1]: Using default value "1" for database type.
```

7 Especifique la información de conexión de la base de datos.

La información que el script requiere depende del tipo de base de datos que elija. Este ejemplo muestra los indicadores que siguen la especificación de una base de datos de Oracle. Los indicadores de otros tipos de bases de datos son similares.

a Especifique el nombre de host o la dirección IP del servidor de base de datos.

```
Enter the host (or IP address) for the database:10.150.10.78
```

b Especifique el puerto de la base de datos o pulse Entrar para aceptar el valor predeterminado.

```
Enter the database port [default=1521]: Using default value "1521" for port.
```

c Especifique el nombre del servicio de base de datos.

```
Enter the database service name [default=oracle]:orcl.example.com
```

Si pulsa Entrar, el script de configuración utiliza un valor predeterminado, el cual podría no ser correcto para algunas instalaciones. Si desea obtener información sobre cómo buscar el nombre del servicio de una base de datos de Oracle, consulte "Configuración de una base de datos de Oracle," página 16.

d Especifique el nombre de usuario y la contraseña de la base de datos.

```
Enter the database username:vcloud
Enter the database password:
```

El script valida la información que ha proporcionado y luego continúa con otros tres pasos.

1 Inicializa la base de datos y conecta este servidor a la misma.

2 Ofrece el inicio de los servicios de vCloud Director en este host.

3 Muestra una dirección URL en la cual se puede conectar al asistente para la instalación después de que se inicie el servicio de vCloud Director.

Este fragmento muestra una finalización típica del script.

```
Connecting to the database: jdbc:oracle:thin:vcloud/vcloud@10.150.10.78:1521/vcloud
...........
Database configuration complete. Once the vCloud Director server has been started you will be
able to access the first-time setup wizard at this URL: http://vcloud.example.com Would you like
to start the vCloud Director service now? If you choose not to start it now, you can manually
start it at any time using this command: service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment). The service was started; it may
be several minutes before it is ready for use. Please check the logs for complete details.
vCloud Director configuration is now complete. Exiting...
```

Qué hacer a continuación

NOTA: La información de conexión de base de datos y otras respuestas reutilizables que haya proporcionado durante la configuración se conservan en un archivo 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. Conserve el archivo en un lugar seguro y ponerlo a disposición solamente cuando sea necesario.

Para agregar más servidores al grupo, consulte "Instalación del software de vCloud Director en miembros adicionales de un grupo de servidores," página 36.

Después de que los servicios de vCloud Director se estén ejecutando en todos los servidores, puede abrir el asistente para la instalación en la dirección URL que se muestra cuando se completa el script. Consulte Capítulo 4, "Configuración de vCloud Director," página 53.

Protección y reutilización del archivo de respuesta

Los detalles de conexión de red y de base de datos que proporciona cuando configura la primera instancia del servidor 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. Conserve el archivo en un lugar seguro y ponerlo a disposición solamente cuando sea necesario.

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 más servidores al grupo, debe utilizar una copia del archivo de respuesta para proporcionar los parámetros de configuración que comparten todos los servidores.

Procedimiento

1 Proteja el archivo de respuesta.

   Guarde una copia del archivo 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 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
   ```

Qué hacer a continuación

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

Instalación del software de vCloud Director en miembros adicionales 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, deberá utilizar el archivo de respuesta que creó al configurar el primer miembro del grupo para proporcionar esta información cuando configure miembros adicionales.

Prerequisitos

- Compruebe que puede acceder al archivo de respuesta que creó cuando instaló y configuró el primer miembro del grupo de servidores. Consulte "Protección y reutilización del archivo de respuesta," página 35.
- Compruebe que se puede acceder a la base de datos de vCloud Director desde este servidor.
- Compruebe que los certificados SSL que ha creado para este servidor estén instalados en una ubicación a la que pueda obtener acceso el instalador. Consulte "Creación e importación de certificados SSL firmados," página 19. El script de configuración no se ejecuta con una identidad privilegiada, por lo que todos los usuarios deben poder leer el archivo del almacén de claves y la ruta en la que está almacenado. El uso de la misma ruta de almacén de claves (por ejemplo, `/tmp/certificates.ks`) en todos los miembros de un grupo de servidores simplifica el proceso de instalación.
- Debe tener la siguiente información disponible:
  - Contraseña del archivo de almacén de claves que incluye los certificados SSL de este servidor.
  - Contraseña de cada certificado SSL.

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 CD o en otro medio, copie el archivo de instalación en una ubicación que sea accesible para todos los servidores 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 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.

5 En una ventana de consola, shell o terminal, ejecute el archivo de instalación utilizando la opción `-r` y especificando el nombre de ruta del archivo de respuesta.

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

```
[root@cell1 /tmp]# ./installation-file -r /path-to-response-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.

El instalador imprime la siguiente advertencia si no ha instalado la clave pública de VMware en el servidor de destino.

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

Cuando se ejecuta el instalador con la opción `-r`, lleva a cabo estas acciones:

a Comprueba que el host cumple todos los requisitos

b Verifica la firma digital del archivo de instalación

c Crea el usuario y grupo `vcloud`

d Desempaqueta el paquete RPM de vCloud Director

e Instala el software

f Copia el archivo de respuesta en una ubicación legible para vcloud.vcloud

g Ejecuta el script de configuración utilizando el archivo de respuesta como entrada

Cuando se ejecuta el script de configuración, busca los certificados en la ruta guardada en el archivo de respuesta (por ejemplo, `/tmp/certificates.ks`) y, a continuación, le solicita que proporcione las contraseñas del almacén de claves y de los certificados. Si el script de configuración no encuentra certificados válidos en el nombre de ruta guardado en el archivo de respuesta, le solicitará un nombre de ruta a los certificados.

6 (Opcional) Repita este procedimiento para añadir más servidores a este grupo de servidores.

Qué hacer a continuación

Si su nube necesita dar soporte a la personalización de invitados para determinados sistemas operativos de Microsoft antiguos, instale archivos de Sysprep en todos los miembros del grupo de servidores. Consulte "Instalar archivos de Microsoft Sysprep en los servidores," página 37.

Después de que finalice el script de configuración y los servicios de vCloud Director se estén ejecutando en todos los servidores, puede abrir el asistente para la instalación en la dirección URL que se muestra cuando se completa el script. Consulte Capítulo 4, "Configuración de vCloud Director," página 53.

Instalar archivos de Microsoft Sysprep en los servidores

Para que vCloud Director pueda realizar una personalización de invitado en máquinas virtuales con determinados sistemas operativos invitados Windows, debe instalar los archivos de Microsoft Sysprep correspondientes 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.

Prerequisitos

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 `$VCLOUD_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 `$VCLOUD_HOME/guestcustomization/default/windows/sysprep`.

Los nombres de subdirectorio son específicos de un sistema operativo invitado.

Tabla 2-1. Asignaciones de subdirectorios para archivos de Sysprep

SO invitado	Subdirectorio para crear en $VCLOUD_HOME/guestcustomization/default/windows/sysprep
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 `vcloud.vcloud`.

Utilice el comando `chown` de Linux para ello.

```
[root@cell1 /]# chown -R vcloud:vcloud $VCLOUD_HOME/guestcustomization
```

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.

Inicio o detención de servicios de vCloud Director

Tras completar la instalación y la configuración de la conexión de base de datos en un servidor, puede iniciar los servicios de vCloud Director en él. También puede detener dichos servicios si se encuentran en ejecución.

El script de configuración le indica que inicie los servicios de vCloud Director. Puede dejar que el script inicie estos servicios, o puede iniciarlos usted mismo más adelante. Los servicios deben estar en ejecución para que pueda finalizar e inicializar la instalación.

Los servicios de vCloud Director se inician siempre que rearranque un servidor.

IMPORTANTE: Si está deteniendo los servicios de vCloud Director como parte de una actualización de software de vCloud Director, deberá utilizar la herramienta de administración de celdas, que le permite poner la celda en modo inactivo antes de detener los servicios. Consulte "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 44.

Procedimiento

1 Inicie sesión en el servidor de destino como raíz.

2 Inicie o detenga los servicios.

Opción	Acción
Iniciar los servicios	Abra una ventana de consola, shell o terminal, y ejecute el comando siguiente. `service vmware-vcd start`
Detenga los servicios cuando se esté utilizando la celda	Utilice la herramienta de administración de celdas.
Detenga los servicios cuando no se esté utilizando la celda	Abra una ventana de consola, shell o terminal, y ejecute el comando siguiente. `service vmware-vcd stop`

Desinstalación del software de vCloud Director

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 `rpm`.

```
rpm -e vmware-vcloud-director
```

Actualización de vCloud Director 3

Para actualizar vCloud Director a una nueva versión, instale la nueva versión en cada servidor del grupo de servidores de vCloud Director, actualice la base de datos de vCloud Director y reinicie los servicios de vCloud Director.

IMPORTANTE: Este procedimiento de actualización da por sentado que usted está actualizando una instalación de vCloud Director que utiliza VMware vSphere y componentes de red (VMware NSX para vSphere o VMware vCloud Networking and Security) compatibles con vCloud Director8.0. Antes de comenzar con el procedimiento, consulte *VMware Product Interoperability Matrixes* en http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php para obtener información sobre las versiones de otros productos de VMware compatibles con la versión de vCloud Director que está utilizando y con vCloud Director 8.0. Puede que sea necesario actualizar algunos de los componentes en de su instalación actual de vCloud Director para obtener las versiones compatibles con vCloud Director 8.0.

Después de actualizar un servidor de vCloud Director, también debe actualizar su 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 asegurarse de que no permanezca ninguna información de tarea no válida en la base de datos después de la actualización, debe asegurarse de que ninguna tarea esté activa en el 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 en la personalización de invitados se copian en la nueva instalación.

A no ser que utilice un equilibrador de carga para distribuir las solicitudes de los clientes entre los miembros de su grupo de servidores de vCloud Director(consulte "Uso de un equilibrador de carga para reducir el tiempo de inactividad del servicio," página 42), la actualización requiere un tiempo de inactividad de vCloud Director suficiente para actualizar la base de datos y, como mínimo, un servidor.

Actualización de un grupo de servidores de vCloud Director

1. Deshabilite el acceso de los usuarios a vCloud Director. También puede mostrar un mensaje de mantenimiento mientras se está produciendo la actualización. Consulte "Visualización del mensaje de mantenimiento durante una actualización," página 43.
2. Utilice la herramienta de administración de celdas para poner todas las celdas del grupo de servidores en modo inactivo y apagar los servicios de vCloud Director en cada servidor. Consulte "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 44.

3 Actualice el software de vCloud Director en todos los miembros del grupo de servidores. Consulte "Actualización del software de vCloud Director en cualquier miembro de un grupo de servidores," página 45. Puede actualizar los servidores de forma individual o en paralelo, pero no debe reiniciar los servicios de vCloud Director en ningún miembro del grupo actualizado antes de actualizar la base de datos de vCloud Director.

4 Actualice la base de datos de vCloud Director. Consulte "Actualización de la base de datos de vCloud Director," página 48.

5 Reinicie vCloud Director en los servidores actualizados. Consulte "Inicio o detención de servicios de vCloud Director," página 38.

6 Habilite el acceso de los usuarios a vCloud Director.

7 (Opcional) Actualice cada versión asociada de vShield Manager o NSX Manager. Todas las instalaciones de vShield Manager o NSX Manager registradas en este grupo de servidores deben actualizarse a una versión del software de vShield Manager o NSX Manager que sea compatible con la versión de vCloud Director instalada por la actualización. Si el programa de actualización detecta una versión incompatible de vShield Manager o NSX Manager, no se permite la actualización. Debe actualizarse a la versión de vShield Manager o NSX Manager más reciente como se describe en "Plataformas compatibles," página 9 para utilizar las funciones de red que se presentan en esta versión de vCloud Director. Consulte "Actualización de una versión de vShield Manager o NSX Manager existente asociada a un sistema vCenter Server adjunto," página 49.

8 (Opcional) Actualice cada sistema de vCenter Server y hosts asociados. Consulte "Actualización de sistemas vCenter Server, hosts y dispositivos de vShield Edge," página 51. Todos los sistemas vCenter Server registrados en este grupo de servidores deben actualizarse a una versión de software de vCenter Manager que sea compatible con la versión de vCloud Director instalada por la actualización. Una vez completada la actualización de vCloud Director, no se podrá acceder a los sistemas vCenter Server no compatibles. Consulte "Plataformas compatibles," página 9.

NOTA: Al finalizar la actualización, si tiene la consola web de vCloud Director abierta en un explorador, cierre sesión y borre la caché del explorador antes de volver a iniciar sesión en la consola web.

Uso de un equilibrador de carga para reducir el tiempo de inactividad del servicio

Si utiliza un equilibrador de carga u otra herramienta que pueda forzar las solicitudes para que vayan a servidores específicos, puede actualizar un subconjunto del grupo de servidores mientras mantiene disponibles los servicios en el subconjunto restante. Este método reduce el tiempo de inactividad del servicio de vCloud Director al lapso de tiempo necesario para actualizar la base de datos de vCloud Director. Es posible que los usuarios experimenten una degradación del rendimiento durante la actualización, pero las tareas en curso seguirán ejecutándose siempre que se mantenga operativo algún subconjunto del grupo de servidores. Tal vez se interrumpan las sesiones de consola, pero puede reiniciarlas.

1 Utilice el equilibrador de carga para redirigir las solicitudes de vCloud Director a un subconjunto de los servidores del grupo. Siga los procedimientos recomendados por el equilibrador de carga.

2 Utilice la herramienta de administración de celdas para poner en modo inactivo las celdas que ya no estén procesando solicitudes y apagar los servicios de vCloud Director en esos servidores.

NOTA: Las sesiones de consola enrutadas a través del proxy de consola del servidor se interrumpen cuando se cierra el servidor. Los clientes pueden actualizar la ventana de la consola para recuperar.

Consulte "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 44.

3 Actualice el software de vCloud Director en los miembros del grupo de servidores en los cuales haya detenido vCloud Director, pero no reinicie dichos servicios. Consulte "Actualización del software de vCloud Director en cualquier miembro de un grupo de servidores," página 45.

4 Utilice la herramienta de administración de celdas para poner en modo inactivo las celdas que aún no haya actualizado y apagar los servicios de vCloud Director en esos servidores.

5 Actualice la base de datos de vCloud Director. Consulte "Actualización de la base de datos de vCloud Director," página 48.

6 Reinicie vCloud Director en los servidores actualizados. Consulte "Inicio o detención de servicios de vCloud Director," página 38.

7 (Opcional) Actualice cada versión asociada de vShield Manager o NSX Manager. Consulte "Actualización de una versión de vShield Manager o NSX Manager existente asociada a un sistema vCenter Server adjunto," página 49.

8 (Opcional) Actualice cada sistema de vCenter Server y hosts asociados. Consulte "Actualización de sistemas vCenter Server, hosts y dispositivos de vShield Edge," página 51.

9 Utilice el equilibrador de carga para redirigir las solicitudes de vCloud Director a los servidores actualizados.

10 Actualice el software de vCloud Director en los servidores restantes del grupo y reinicie vCloud Director en dichos servidores a medida se completen las actualizaciones. Consulte "Actualización del software de vCloud Director en cualquier miembro de un grupo de servidores," página 45.

Visualización del mensaje de mantenimiento durante una actualización

Si espera que el proceso de actualización sea largo y desea que el sistema muestre un mensaje de mantenimiento mientras se realiza la actualización, asegúrese de que se pueda acceder a una celda como mínimo mientras se actualizan las otras. Ejecute el comando `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` en esa celda para activar el mensaje de mantenimiento de celdas.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
```

Cuando esté listo para devolver una celda actualizada al servicio, ejecute el siguiente comando en la celda para desactivar el mensaje de mantenimiento.

```
[root@cell1 /opt/vmware/vcloud-director/bin]# service vmware-vcd restart
```

Este capítulo cubre los siguientes temas:

Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo

Antes de actualizar un vCloud Director Server, utilice la herramienta de administración de celdas para poner en modo inactivo los servicios de vCloud Director y apagarlos en la celda del servidor.

vCloud Director crea un objeto de tarea para controlar y administrar cada operación asincrónica que el usuario solicite. 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. Debido a que la actualización de la base de datos invalida esta información de la tarea, cerciórese de que no se esté ejecutando ninguna tarea antes de empezar el proceso de actualización.

Con la herramienta de administración de celdas, puede suspender el programador de tareas a fin de que no se puedan iniciar nuevas tareas, para luego verificar el estado de todas las tareas activas. Puede esperar a que finalicen todas las tareas en ejecución o iniciar sesión en vCloud Director como administrador del sistema y cancelar las mismas. Consulte Capítulo 5, “Referencia de la herramienta de administración de celdas,” página 57. Si no se está ejecutando ninguna tarea, puede utilizar la herramienta de administración de celdas para detener los servicios de vCloud Director.

Prerequisitos

- Verifique que dispone de credenciales de superusuario en el servidor de destino.
- Verifique que dispone de credenciales de administrador del sistema de vCloud Director.
- Si la celda estará accesible para los clientes de vCloud Director mientras se actualiza, utilice el comando `/opt/vmware/vcloud-director/bin/vmware-vcd-cell` para activar el mensaje de mantenimiento de la celda.

  ```
  [root@cell1 /opt/vmware/vcloud-director/bin]# ./vmware-vcd-cell maintenance
  ```

  Este comando hace que la celda responda a todas las solicitudes con un mensaje de mantenimiento. Si utiliza un equilibrador de carga o una herramienta similar para que no pueda accederse a la celda durante la actualización, no tendrá que activar el mensaje de mantenimiento de la celda.

Procedimiento

1 Inicie sesión en el servidor de destino como raíz.

2 Utilice la herramienta de administración de celdas para apagar correctamente la celda.

a Recupere el estado del trabajo actual.

El comando `cell-management-tool` proporciona las credenciales del administrador del sistema y devuelve un recuento de los trabajos en ejecución.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3 Is Active = true
```

b Detenga el programador de tareas para poner la celda en modo inactivo.

Utilice un comando `cell-management-tool` con el siguiente formato.

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

Este comando evita que se inicien nuevos trabajos. Los trabajos existentes se siguen ejecutando hasta que se finalicen o se cancelen. Para cancelar un trabajo, utilice la consola web de vCloud Director o la API REST.

c Cuando el valor de `Job count` es `0` y el de `Is Active` es `false`, es seguro cerrar la celda.

Utilice un comando `cell-management-tool` con el siguiente formato.

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

NOTA: Puede proporcionar la contraseña de administrador del sistema de vCloud Director en la línea de comandos `cell-management-tool`, pero es más seguro omitirla. Esto hace que el comando `cell-management-tool` solicite la contraseña, que no se mostrará en la pantalla según se vaya escribiendo.

Las sesiones de consola enrutadas a través del proxy de consola del servidor se interrumpen cuando se cierra el servidor. Si otros miembros del grupo de servidores siguen estando activos, los clientes podrán actualizar la ventana de la consola para recuperar.

Qué hacer a continuación

Después de que la herramienta de administración de celdas detiene los servicios de vCloud Director en este servidor, puede actualizar el software de vCloud Director del servidor o completar otras tareas de mantenimiento que requiere el servidor.

Actualización del software de vCloud Director en cualquier miembro de un grupo de servidores

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.

El software de vCloud Director se distribuye como archivo ejecutable de Linux denominado `vmware-vcloud-director-8.0.0-`*nnnnnn*`.bin`, donde *nnnnnn* representa el número de compilación. Después de que se instale la actualización en un miembro del grupo de servidores, debe ejecutar una herramienta que actualiza la base de datos de vCloud Director que el grupo utiliza antes de poder reiniciar los servicios de vCloud Director en el servidor actualizado.

Prerequisitos

- Verifique que dispone de credenciales de superusuario en el servidor de destino.

- Para 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," página 27.
- Utilice la herramienta de administración de celdas para poner en modo inactivo y apagar los servicios de vCloud Director en la celda del servidor.
- Verifique que tiene una clave de licencia válida para usar la versión del software de vCloud Director a la que se está actualizando.

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 CD o en otro medio, copie el archivo de instalación en una ubicación que sea accesible para todos los servidores de destino.

3 Compruebe que la suma de comprobación de la descarga coincide 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 coincide con el que aparece 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
checksum-value installation-file
```

Compare el valor *checksum-value* que produce este comando con la suma de comprobación MD5 copiada de la página descargada.

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 Utilice la herramienta de administración de celdas para poner en modo inactivo la celda y apagar los servicios de vCloud Director en el servidor.

Consulte "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 44.

6 Ejecute el archivo de instalación en una ventana de consola, shell o terminal.

Para ejecutar el archivo de instalación, especifique el nombre de ruta completo, por ejemplo `./archivo-de-instalación`. 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 instalada en este servidor que sea igual o posterior a la versión del archivo de instalación, muestra un mensaje de error y sale. En caso contrario, le pide que confirme que está listo para actualizar el servidor.

```
Checking architecture...done
Checking for a supported Linux distribution...done
Checking for necessary RPM prerequisites...done
Checking free disk space...done
An older version of VMware vCloud Director has been detected
```

7 Responda al indicador de actualización.

Opción	Acción
Continuar la actualización.	Escriba **y**.
Salir del shell sin realizar ningún cambio en la instalación actual.	Escriba **n**.

Tras confirmar que está listo para actualizar el servidor, el instalador verifica que el host cumpla todos los requisitos, abre el paquete RPM de vCloud Director, detiene los servicios de vCloud Director en el servidor y actualiza el software de vCloud Director que esté instalado.

```
Do you wish to proceed with the upgrade? (y/n)? y
Extracting vmware-vcloud-director ......done
Upgrading VMware vCloud Director...
Installing the VMware vCloud Director
Preparing...                ##################################################
vmware-vcloud-director      ##################################################
Migrating settings and files from previous release...done
Migrating in-progress file transfers to /opt/vmware/vcloud-director/data/transfer...done
Uninstalling previous release...done
```

El instalador muestra la siguiente advertencia si no ha instalado la clave pública de VMware en el servidor de destino.

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

El instalador muestra la siguiente advertencia cuando efectúa cambios en el archivo `global.properties` del servidor de destino.

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

La mayoría de las actualizaciones requieren este tipo de cambio y muestran esta advertencia. Si ha hecho muchos cambios en el archivo `global.properties`, puede recuperarlos de `global.properties.rpmnew`.

8 (Opcional) Actualice las propiedades de registro.

Después de una actualización, las nuevas propiedades de registro se escriben en el archivo `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew`.

Opción	Acción
Si no ha cambiado las propiedades de registro existentes	Copie este archivo en `/opt/vmware/vcloud-director/etc/log4j.properties`.
Si ha cambiado las propiedades de registro	Combine el archivo `/opt/vmware/vcloud-director/etc/log4j.properties.rpmnew` con el archivo `/opt/vmware/vcloud-director/etc/log4j.properties` existente. Al combinar estos archivos se mantienen los cambios.

Una vez que finaliza la actualización del software de vCloud Director, el instalador muestra un mensaje que indica dónde están almacenados los archivos de configuración anteriores y luego le recuerda que ejecute la herramienta de actualización de la base de datos.

Qué hacer a continuación

- Si aún no lo ha hecho, actualice la base de datos de vCloud Director que este servidor utiliza.
- Si ya actualizó la base de datos de vCloud Director que utiliza este grupo de servidores, puede reiniciar el servidor actualizado. Consulte "Inicio o detención de servicios de vCloud Director," página 38.

Actualización de la base de datos de vCloud Director

Después de actualizar un servidor en el grupo de servidores de vCloud Director, debe actualizar la base de datos de vCloud Director del grupo para poder reiniciar los servicios de vCloud Director en el servidor.

Todos los servidores de un grupo de servidores de vCloud Director comparten la misma base de datos; por eso, independientemente del número de servidores que vaya a actualizar, solo tendrá que actualizar la base de datos una vez. Una vez actualizada la base de datos, los servidores de vCloud Director no se podrán conectar a ella hasta que no se hayan actualizado también.

Prerequisitos

IMPORTANTE: Cree una copia de seguridad de la base de datos existente antes de actualizarla. Utilice los procedimientos que el proveedor del software de base de datos recomienda.

Compruebe que todas las celdas de vCloud Director estén inactivas. Véase "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 44

Procedimiento

1 Abra una ventana de consola, shell o terminal, y escriba el comando siguiente para ejecutar el script de actualización de base de datos.

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

IMPORTANTE: Si el script de actualización de base de datos detecta que se ha registrado una versión incompatible de vShield Manager o NSX Manager en esta instalación de vCloud Director, muestra este mensaje de aviso y cancela la actualización.

```
One or more vShield Manager servers registered to this vCloud Director installation are not
supported by the version of vCloud Director you are upgrading to. Upgrade canceled, please
follow the procedures in the vShield Manager Upgrade Guide to upgrade those unsupported
vShield Manager servers.
```

2 Responda a los indicadores de actualización de base de datos.

a Confirme que desea continuar con la actualización de la base de datos.

```
Welcome to the vCloud Director upgrade utility This product is intended for use only by
service providers under the terms and conditions of the VMware Service Provider Partner
(VSPP) Program. If you are a member of the VSPP Program, please locate your license key
before proceeding. If you are not a member of this program, do not proceed with this
upgrade. Upgrading without a proper key will invalidate your support contract. Esta
función aplicará varias actualizaciones a la base de datos. Please ensure you have
created a backup of your database prior to continuing. ¿Desea actualizar ahora? [Y/N]:
```

Lleve a cabo una de las siguientes acciones:

Opción	Acción
Continuar la actualización.	Escriba **y**.
Salir del shell sin realizar ningún cambio en la base de datos de vCloud Director actual.	Escriba **n**.

b (Opcional) Espere a que las celdas pasen a estar inactivas, si es necesario.

Si la herramienta de actualización de base de datos detecta que hay todavía alguna celda activa, le preguntará si desea continuar con la actualización o salir.

```
Found active cell. Name: "cell-01", IP Address: 10.150.151.190, Identifier: a2eb...
Do you wish to upgrade the database while cells are still active? [Y/N]
```

Si se muestra este indicador, escriba `n` para salir del shell, espere cinco minutos y reinicie la herramienta de actualización de base de datos. Si la herramienta de actualización de base de datos sigue advirtiéndole de que hay todavía celdas activas, vuelva al procedimiento incluido en "Uso de la herramienta de administración de celdas para poner un servidor en modo inactivo o apagarlo," página 44 y compruebe que todas las celdas hayan pasado a estar inactivas.

Después de que haya respondido a todos los indicadores, la herramienta de actualización de base de datos se ejecuta y muestra mensajes del progreso.

```
Executing upgrade task: Start UpdateStatementManager ...[3] Successfully ran upgrade task
Executing upgrade task: ... .......... Successfully ran upgrade task ... Executing upgrade
task: Stop UpdateStatementManager ...[3] ... Successfully ran upgrade task
```

Una vez actualizada la base de datos, el script de actualización ofrecerá iniciar los servicios de vCloud Director en este host.

```
Would you like to start the vCloud Director service now? If you choose not to start it now, you
can manually start it at any time using this command: service vmware-vcd start
Start it now? [y/n]:y
Starting the vCloud Director service (this may take a moment). Iniciando vmware-vcd-watchdog:
[ OK ] Iniciando vmware-vcd-cell [ OK ]
```

Actualización de una versión de vShield Manager o NSX Manager existente asociada a un sistema vCenter Server adjunto

Antes de actualizar un sistema vCenter Server y los hosts adjuntos a vCloud Director, debe actualizar la versión de vShield Manager o NSX Manager asociada con dicho sistema vCenter Server.

La actualización de vShield Manager o NSX Manager interrumpe el acceso a las funciones administrativas de vShield Manager o NSX Manager, pero no interrumpe los servicios de red.

Prerequisitos

- Verifique que por lo menos una celda actualizada de su instalación de vCloud Director esté ejecutándose antes de iniciar la actualización. La celda escribe datos sobre la actualización de vShield Manager o NSX Manager en la base de datos de vCloud Director.
- Verifique que tiene todos los elementos necesarios para actualizar vShield Manager o NSX Manager, en función de lo que esté actualizando.

vShield Manager	NSX Manager
Consulte la información de actualización disponible en el Centro de documentación de VMware vCloud Networking and Security en https://www.vmware.com/support/pubs/vshield_pubs.html.	Consulte la información de actualización disponible en el Centro de documentación de NSX for vSphere en https://www.vmware.com/support/pubs/nsx_pubs.html.

Procedimiento

1 Actualice la instalación asociada de vShield Manager o NSX Manager siguiendo el procedimiento correspondiente al producto y a la versión a los que está actualizando.

ADVERTENCIA: Cuando actualiza a una versión de NSX Manager, no actualice los dispositivos de vShield Edge asociados existentes a dispositivos de NSX Edge. vCloud Director no admite dispositivos de NSX Edge. Cuando se usa NSX Manager con vCloud Director, vCloud Director utiliza NSX Manager para crear dispositivos de vShield Edge.

Opción	Acción
Actualice una versión de vShield Manager asociada a una versión posterior de vShield Manager.	Consulte la información sobre la actualización de vShield Manager en la *Guía de instalación y actualización de vShield* en https://www.vmware.com/support/pubs/vshield_pubs.html. Actualice vShield Manager únicamente y no otros componentes de vShield. No actualice los dispositivos asociados de vShield Edge existentes.
Actualice una versión de vShield Manager asociada a NSX Manager, o actualice una versión de NSX Manager asociada a una versión de NSX Manager posterior.	Consulte la información sobre la actualización de NSX Manager en la *Guía de instalación y actualización de NSX* en https://www.vmware.com/support/pubs/nsx_pubs.html. Actualice vShield Manager o NSX Manager únicamente y no otros componentes de vShield o NSX for vSphere. No actualice los dispositivos asociados de vShield Edge existentes.

2 Repita Step 1 con cada vShield Manager o NSX Manager asociado con los demás sistemas de vCenter Server registrados en su nube.

Una vez que la actualización finaliza, la versión actualizada de vShield Manager o NSX Manager notifica a vCloud Director que el software está en una nueva versión. Pueden pasar varios minutos hasta que se envía la notificación y vCloud Director la procesa.

Qué hacer a continuación

Después de actualizar cada versión asociada de vShield Manager o NSX Manager, debe actualizar todos los sistemas vCenter Server y hosts registrados antes de utilizar vCloud Director para actualizar los dispositivos de vShield Edge asociados. Consulte "Actualización de sistemas vCenter Server, hosts y dispositivos de vShield Edge," página 51.

Actualización de sistemas vCenter Server, hosts y dispositivos de vShield Edge

Después de actualizar vCloud Director y vShield Manager o NSX Manager, debe actualizar los hosts y los sistemas vCenter Server adjuntos a su nube. Una vez que todos los hosts y sistemas vCenter Server están actualizados, debe usar vCloud Director para actualizar los dispositivos de vShield Edge asociados volviendo a implementar las puertas de enlace Edge o restableciendo las redes vApp.

Prerequisitos

Verifique que ya ha actualizado cada vShield Manager o NSX Manager asociado a los sistemas vCenter Server adjuntos a su nube. Consulte "Actualización de una versión de vShield Manager o NSX Manager existente asociada a un sistema vCenter Server adjunto," página 49.

Procedimiento

1 Actualice el sistema vCenter Server adjunto.

   Consulte la *Guía de instalación y configuración de vSphere*.

2 Verifique todas las URL públicas de vCloud Director y las cadenas de los certificados.

   En la pestaña **Administración** de la consola web de vCloud Director, haga clic en **Direcciones públicas** en el panel izquierdo. Escriba valores en todos los campos.

3 (Opcional) Si ha configurado vCloud Director para utilizar el inicio de sesión único de vCenter, deberá anular el registro de vCloud Director y volver a registrarlo en el servicio de búsqueda de vCenter.

   a Inicie sesión en vCloud Director como administrador del sistema utilizando una cuenta local o LDAP. No utilice el inicio de sesión único de vCenter para este inicio de sesión.

   b Anule el registro de vCloud Director en el servicio de búsqueda de vCenter.

      En la pestaña **Administración** de la consola web de vCloud Director, haga clic en **Federación** en el panel izquierdo y después en **Anular registro**. Para completar esta acción, deberá proporcionar las credenciales de administrador de vCenter correctas.

   c Registre vCloud Director en el servicio de búsqueda de vCenter.

      Consulte el apartado "Configurar vCloud Director para utilizar el inicio de sesión único de vCenter" en la *Guía del administrador de vCloud Director*.

4 Actualice el registro del sistema vCenter Server con vCloud Director.

   a En la consola web de vCloud Director, haga clic en la pestaña **Administrar y supervisar** y haga clic en **vCenters** en el panel izquierdo.

   b Haga clic con el botón secundario en el nombre de vCenter Server y seleccione **Actualizar**.

   c Haga clic en **Sí**.

5 Actualice los hosts compatibles con el sistema vCenter Server actualizado.

   Consulte la *Guía de instalación y configuración de vSphere*. Con cada host, la actualización requiere los siguientes pasos:

   a En la consola web de vCloud Director, deshabilite el host.

      En la página **Gestionar y Supervisar**, haga clic en **Hosts** y, a continuación, haga clic con el botón secundario y seleccione **Deshabilitar host**.

   b 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.

c Actualice el host.

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.

d Use el sistema vCenter Server para volver a conectar el host.

e Actualice el agente de host de vCloud Director en el host.

Consulte el apartado "Actualizar un agente de host ESX/ESXi" en la *Guía del administrador de vCloud Director*.

f En la consola web de vCloud Director, habilite el host.

En la página **Gestionar y Supervisar**, haga clic en **Hosts** y, a continuación, haga clic con el botón secundario y seleccione **Habilitar host**.

g Utilice el sistema vCenter Server para finalizar el modo de mantenimiento del host.

6 Use su versión de vCloud Director actualizada para actualizar todos los dispositivos de vShield Edge administrados por la versión actualizada de vShield Manager o NSX Manager asociado con el sistema vCenter Server actualizado.

ADVERTENCIA: Si el sistema vCenter Server actualizado está asociado con NSX Manager en lugar de con vShield Manager, utilice únicamente los métodos descritos en este paso para actualizar automáticamente los dispositivos de vShield Edge usando vCloud Director. No utilice ningún otro método para actualizar los dispositivos de vShield Edge asociados a dispositivos de NSX Edge. vCloud Director no admite dispositivos de NSX Edge. Cuando se usa NSX Manager con vCloud Director, vCloud Director utiliza NSX Manager para crear dispositivos de vShield Edge.

La actualización correspondiente de un dispositivo de vShield Edge se produce de manera automática cuando se utiliza la consola web de vCloud Director o REST API para restablecer una red que protege vShield Edge.

- En el caso de las puertas de enlace Edge, cuando se implementa de nuevo la puerta de enlace Edge, se actualiza el dispositivo de vShield Edge asociado con ella.
- Para las redes vApp con las que se conectan las máquinas virtuales, como las redes vApp enrutadas, las redes vApp aisladas o las redes con barrera de centros de datos virtuales de organización, restablecer la red vApp desde el interior del contexto de la vApp actualiza el dispositivo de vShield Edge asociado con dicha red. Si desea usar la consola web de vCloud Director para restablecer una red de vApp desde el interior del contexto de una vApp, desplácese hasta la pestaña **Redes** de la vApp, muestre sus detalles de red, haga clic con el botón secundario del ratón en la red de vApp y seleccione **Restablecer red**.

Para obtener más información sobre cómo implementar de nuevo las puertas de enlace Edge y restablecer las redes de vApp, consulte la vCloud Directorayuda en línea de la consola web o la *Guía de programación de vCloud API*, en función del método que vaya a emplear.

Qué hacer a continuación

Repita este procedimiento con los demás sistemas vCenter Server registrados en su nube.

Configuración de vCloud Director 4

Después de configurar todos los servidores del grupo de servidores de vCloud Director y de conectarlos a la base de datos, puede inicializar la base de datos del grupo de servidores con una clave de licencia, una cuenta de administrador del sistema y la información asociada. Una vez que finalice este proceso, puede utilizar la consola web de vCloud Director para completar el aprovisionamiento de la nube.

Para poder ejecutar la consola web de vCloud Director, debe ejecutar el asistente para configuración, el cual recopila la información que la consola web requiere para poder iniciarse. Después de que finalice el asistente, la consola web se inicia y muestra la pantalla de inicio de sesión. La consola web de vCloud Director proporciona un conjunto de herramientas para el aprovisionamiento y la administración de nubes. Incluye una función de inicio rápido que le guía por pasos, como la forma de adjuntar vCloud Director a vCenter y de crear una organización.

Prerequisitos

- Complete la instalación de todos los vCloud Director Servers y verifique que los servicios de vCloud Director se hayan iniciado en todos los servidores.
- Verifique que tenga la dirección URL que el script de configuración muestra cuando finaliza.

  NOTA: Para averiguar la dirección URL del asistente para configuración después de que salga el script, busque el nombre de dominio totalmente cualificado con la dirección IP que especificó para el servicio HTTP durante la instalación del primer servidor y utilícelo para construir una dirección URL con el formato https://*nombre-de-dominio-totalmente-cualificado*, por ejemplo, https://minube.ejemplo.com. Puede conectarse con el asistente en esa dirección URL.

Complete la instalación de todos los vCloud Director Servers y verifique que los servicios de vCloud Director se hayan iniciado en todos los servidores.

Procedimiento

1 Abra un explorador web y conéctese a la dirección URL que el script de configuración muestra cuando finaliza.

  NOTA: Después de iniciar los servicios de vCloud Director, es posible que deba esperar algunos minutos a que el asistente para configuración o la consola web estén listos.

2 Siga las indicaciones para completar la configuración.

Este capítulo cubre los siguientes temas:

Lectura del contrato de licencia

Para poder configurar un grupo de servidores de vCloud Director debe leer y aceptar el contrato de licencia de usuario final.

Procedimiento

1 Lea el contrato de licencia.

2 Acepte o rechace el contrato.

Opción	Acción
Para aceptar el contrato de licencia.	Haga clic en **Sí, acepto los términos del contrato de licencia**.
Para rechazar el contrato de licencia.	**No, no acepto los términos del contrato de licencia**.

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

Especificación de la clave de licencia

Cada clúster de vCloud Director requiere una licencia para su ejecución. La licencia se especifica a modo de número de serie de producto. El número de serie de producto se almacena en la base de datos de vCloud Director.

El número de serie de producto de vCloud Director no es el mismo que la clave de licencia del vCenter Server. Para utilizar vCloud, debe disponer de un número de serie de producto de vCloud Director y de una clave de licencia de vCenter Server. Puede obtener ambos tipos de claves de licencia en el Portal de licencias de VMware.

Procedimiento

1 Obtenga un número de serie de producto de vCloud Director en el Portal de licencias de VMware.

2 Especifique el número de serie de producto en el cuadro de texto **Número de serie del producto**.

Creación de una cuenta de administrador del sistema

Especifique el nombre de usuario, la contraseña y la información de contacto del administrador del sistema de vCloud Director.

El administrador del sistema de vCloud Director tiene privilegios de superusuario en toda la nube. La cuenta inicial de administrador del sistema se crea durante la instalación de vCloud Director. Tras completar la instalación y configuración, el administrador del sistema puede crear otras cuentas de administrador como sea necesario.

Procedimiento

1 Especifique el nombre de usuario del administrador del sistema.

2 Especifique la contraseña del administrador del sistema y confírmela.

3 Especifique el nombre completo del administrador del sistema.

4 Especifique la dirección de correo electrónico del administrador del sistema.

Especificación de la configuración del sistema

Puede especificar la configuración del sistema que controla la forma en que vCloud Director interactúa con vSphere y vShield Manager o NSX Manager.

El proceso de configuración crea una carpeta en el sistema vCenter Server para que la utilice vCloud Director y especifica el Id. de instalación que se debe utilizar al crear direcciones MAC para NIC virtuales.

Procedimiento

1 Especifique el nombre de la carpeta de vCloud Director vCenter Server en el campo **Nombre del sistema**.

2 Utilice el campo **Id. de instalación** para especificar el Id. de esta instalación de vCloud Director.

Si el centro de datos incluye varias instalaciones de vCloud Director, cada instalación debe especificar un Id. de instalación único.

Listo para iniciar sesión en vCloud Director

Después de proporcionar toda la información que requiera el asistente para la configuración, puede confirmar los ajustes configurados y finalizar el asistente. Una vez que finalice el asistente, se abre la pantalla de inicio de sesión de la consola web de vCloud Director.

La página Listo para iniciar sesión enumera todos los ajustes de configuración que ha proporcionado al asistente. Examínelos detenidamente.

Prerequisitos

Verifique que tiene acceso al sistema vCenter Server que va a usar con la nube y a vShield Manager o NSX Manager asociado al sistema vCenter Server. La consola web de vCloud Director requiere el acceso a las instalaciones de vCenter Server y vShield Manager o NSX Manager que desee configurar como parte de esta instalación de vCloud Director. Dichas instalaciones deben estar en ejecución y se deben haber configurado de modo que puedan trabajar una con la otra antes de que finalice esta tarea. Para obtener más información sobre los requisitos de configuración, consulte "Requisitos de hardware y software de vCloud Director," página 9.

Procedimiento

- Para cambiar algún valor, haga clic en **Atrás** hasta que llegue a la página donde se haya originado el valor.
- Para confirmar todos los ajustes de configuración y completar el proceso de configuración, haga clic en **Finalizar**.

Al hacer clic en **Finalizar**, el asistente aplica la configuración que haya especificado y luego inicia la consola web de vCloud Director y muestra la pantalla de inicio de sesión.

Qué hacer a continuación

Use la pantalla de inicio de sesión mostrada para iniciar sesión en la consola web de vCloud Director con el nombre de usuario y la contraseña que proporcionó para la cuenta del administrador del sistema. Después de iniciar sesión, la consola muestra un conjunto de pasos de inicio rápido que debe completar antes de utilizar la nube. Una vez que finalice los pasos, se habilitan las Tareas guiadas y la nube está lista para utilizarse.

Referencia de la herramienta de administración de celdas 5

La herramienta de administración de celdas es una utilidad de línea de comandos que puede utilizar para gestionar una celda y sus certificados SSL, así como para exportar tablas de la base de datos de vCloud Director. Se necesitan credenciales de superusuario o de administrador del sistema para realizar algunas operaciones.

La herramienta de administración de celdas se instala en `/opt/vmware/vcloud-director/bin/cell-management-tool`.

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
```

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

```
[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
ciphers - Reconfigure the list of disallowed SSL ciphers for the cell
configure-metrics - Collects and stores properties necessary for collecting and querying metrics
data
dbextract - Exports the data from the given set of tables
fix-scheduler-data - Scan database for corrupt scheduler data.  Fix scheduler job data if
corrupt.
generate-certs - Generates self-signed SSL certificates for use with vCD cell.
recover-password - Change a forgotten System Administrator password. Database credentials are
required.
fail-tasks - Fail all tasks running on this cell and set a custom failure message.

For command specific help:
 cell-management-tool <commandName> -h
```

- Administrar una celda página 59

  Utilice el comando `cell` de la herramienta de administración de celdas para suspender el programador de tareas a fin de que no se puedan iniciar nuevas tareas, para verificar el estado de las tareas activas, para controlar el modo de mantenimiento de las celdas y para cerrar la celda correctamente.

- Exportar tablas de bases de datos página 60

  Utilice el comando `dbextract` de la herramienta de administración de celdas para exportar datos de la base de datos de vCloud Director.

- Detectar y reparar datos dañados del programador página 62

  Si conoce el nombre de usuario y la contraseña de la base de datos de vCloud Director, utilice el comando `fix-scheduler-data` de la herramienta de administración de celdas para buscar datos dañados del programador en la base de datos y repararlos según sea necesario.

- Reemplazo de certificados SSL página 63

  Utilice el comando `certificates` de la herramienta de administración de celdas para sustituir los certificados SSL de la celda.

- Generación de certificados SSL de autofirma página 64

  Utilice el comando `generate-certs` de la herramienta de administración de celdas para generar certificados SSL de firma automática para la celda.

- Administrar la lista de cifrados SSL permitidos página 66

  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 página 68

  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.

- Configuración de la conexión de la base de datos de métricas página 69

  Utilice el comando `configure-metrics` de la herramienta de administración de celdas para conectar con la base de datos de métricas opcional.

- Recuperación de la contraseña del administrador del sistema página 69

  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 página 70

  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 las celdas fueron cerradas deliberadamente. No puede utilizar el comando `fail-tasks` hasta que todas las celdas se hayan cerrado.

Administrar una celda

Utilice el comando `cell` de la herramienta de administración de celdas para suspender el programador de tareas a fin de que no se puedan iniciar nuevas tareas, para verificar el estado de las tareas activas, para controlar el modo de mantenimiento de las celdas y para cerrar la celda correctamente.

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

`cell-management-tool -u` *`sysadmin-nombreUsuario`* `-p` *`sysadmin-contraseña`* `cell` *`comando`*

sysadmin-nombreUsuario Nombre de usuario de un administrador del sistema de vCloud Director.

sysadmin-contraseña Contraseña del administrador del sistema de vCloud Director.

NOTA: Puede proporcionar la contraseña de administrador del sistema de vCloud Director en la línea de comandos `cell-management-tool`, pero es más seguro omitirla. Esto hace que el comando `cell-management-tool` solicite la contraseña, que no se mostrará en la pantalla según se vaya escribiendo.

comando Subcomando `cell`.

Tabla 5-1. Opciones y argumentos de la herramienta de administración de celdas, subcomando `cell`

Comando	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--maintenance` (`-m`)	`true` o `false`	Controla el modo de mantenimiento de las celdas. El argumento `true` coloca la celda en el modo de mantenimiento. (Debe poner la celda en modo inactivo primero.) El argumento `false` libera la celda del modo de mantenimiento.
`--quiesce` (`-q`)	`true` o `false`	Pone la celda en modo inactivo. El argumento `true` suspende el programador. El argumento `false` reinicia el programador.
`--shutdown` (`-s`)	Ninguno	Apaga los servicios de vCloud Director en el servidor.
`--status` (`-t`)	Ninguno	Muestra información en cuanto al número de tareas que se ejecutan en la celda y el estado de ésta.
`--status-verbose` (`-tt`)	Ninguno	Muestra información sobre el número de tareas que se ejecutan en la celda y el estado de ésta.

Ejemplo: Obtener el estado de una tarea

La línea de comandos `cell-management-tool` proporciona las credenciales del administrador del sistema y devuelve un recuento de las tareas en ejecución. Cuando el valor de `Job count` es `0` y el de `Is Active` es `false`, puede cerrar la celda de manera segura.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool -u administrator cell --status
Job count = 3 Is Active = true In Maintenance Mode = false
```

Exportar tablas de bases de datos

Utilice el comando `dbextract` de la herramienta de administración de celdas para exportar datos de la base de datos de vCloud Director.

Para exportar tablas de bases de datos, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool dbextract options
```

Tabla 5-2. Opciones y argumentos de la herramienta de administración de celdas, subcomando `dbextract`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`-categories`	Lista separada por comas de categorías de tabla para exportar.	Opcional. `NETWORKING` es la única categoría compatible
`-dataFile`	Ruta absoluta a un archivo que describe los datos para exportar.	Opcional. Si no se suministra, el comando utiliza `$VCLOUD_HOME/etc/data_to_export.properties`. Consulte "Especificación de tablas y columnas para exportar," página 61.
`-dumpFolder`	Ruta absoluta a la carpeta en la que se crea el volcado. La carpeta debe existir y vcloud.vcloud debe poder escribir en ella.	Todos los datos se exportarán a un archivo de esta carpeta.
`-exportSettingsFile`	Ruta absoluta a un archivo de propiedades de configuración de exportación de datos.	Opcional. Si no se suministra, el comando utiliza `$VCLOUD_HOME/etc/data_export_settings.ini`. Consulte "Limitación y ordenación de las filas exportadas," página 62.
`-properties`	Ruta absoluta a un archivo de propiedades de conexión de base de datos.	Opcional. Si no se suministra, el comando utiliza `$VCLOUD_HOME/etc/global.properties`. Consulte "Especificación de un archivo de propiedades," página 61.
`-tables`	Lista separada por comas de tablas.	Opcional. Exporte todas las tablas para ver los nombres de tabla individuales.

Especificación de un archivo de propiedades

El comando `dbextract` extrae, de forma predeterminada, datos de la base de datos de vCloud Director utilizando la información de conexión de base de datos incluida en el archivo `$VCLOUD_HOME/etc/global.properties` de la celda actual. Para extraer datos de una base de datos de vCloud Director diferente, especifique las propiedades de conexión de base de datos en un archivo y utilice la opción `–properties` para proporcionar el nombre de ruta de ese archivo en la línea de comandos. El archivo de propiedades es un archivo UTF-8 con el siguiente formato.

```
username=username
password=password
servicename=db_service_name
port=db_connection_port
database-ip=db_server_ip_address
db-type=db_type
```

username	El nombre de usuario de la base de datos de vCloud Director.
password	La contraseña de la base de datos de vCloud Director.
db_service_name	Nombre del servicio de base de datos. Por ejemplo, `orcl.example.com`.
db_connection_port	Puerto de la base de datos.
db_server_ip_address	Dirección IP del servidor de base de datos.
db_type	Tipo de la base de datos. Debe ser `Oracle` o `MS_SQL`.

Especificación de tablas y columnas para exportar

Para restringir el conjunto de datos exportados, utilice la opción `–exportSettingsFile` para crear un archivo `data_to_export.properties` que especifique tablas individuales y, opcionalmente, columnas para exportar. Es un archivo UTF-8 que contiene cero o más líneas con el formato *NOMBRE_TABLA*:*NOMBRE_COLUMNA*.

TABLE_NAME	Nombre de una tabla de la base de datos. Para ver una lista de nombres de tabla, exporte todas las tablas.
COLUMN_NAME	El nombre de una columna en el *NOMBRE_TABLA* especificado.

En este ejemplo, el archivo `data_to_export.properties` exporta columnas de las tablas `ACL` y `ADDRESS_TRANSLATION`.

```
ACL:ORG_MEMBER_ID
ACL:SHARABLE_ID
ACL:SHARABLE_TYPE
ACL:SHARING_ROLE_ID
ADDRESS_TRANSLATION:EXTERNAL_ADDRESS
ADDRESS_TRANSLATION:EXTERNAL_PORTS
ADDRESS_TRANSLATION:ID
ADDRESS_TRANSLATION:INTERNAL_PORTS
ADDRESS_TRANSLATION:NIC_ID
```

El comando espera encontrar este archivo en `$VCLOUD_HOME/etc/data_to_export.properties`, pero puede especificar otra ruta si lo desea.

Limitación y ordenación de las filas exportadas

Con cualquier tabla, puede especificar cuántas filas desea exportar y cómo ordenar las filas exportadas. Utilice la opción `–exportSettingsFile` para crear un archivo `data_export_settings.ini` que especifique tablas individuales. Es un archivo UTF-8 que contiene cero o más entradas con el siguiente formato:

```
[TABLE_NAME]
rowlimit=int
orderby=COLUMN_NAME
```

TABLE_NAME Nombre de una tabla de la base de datos. Para ver una lista de nombres de tabla, exporte todas las tablas.

COLUMN_NAME El nombre de una columna en el *NOMBRE_TABLA* especificado.

En este ejemplo el archivo `data_export_settings.ini` limita los datos exportados de la tabla `AUDIT_EVENT` a las primeras 10.000 filas y las ordena según el valor de la columna `event_time`.

```
[AUDIT_EVENT]
rowlimit=100000
orderby=event_time
```

El comando espera encontrar este archivo en `$VCLOUD_HOME/etc/data_export_settings.ini`, pero puede especificar otra ruta si lo desea.

Ejemplo: Exportación de todas las tablas de la base de datos actual de vCloud Director .

En este ejemplo, se exportan todas las tablas de la base de datos actual de vCloud Director al archivo `/tmp/dbdump` .

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool dbextract -dumpFolder /tmp/dbdump
This utility outputs data from your vCloud Director system that may contain sensitive data. Do
you want to continue and output the data (y/n)?
y
Exporting data now. Please wait for the process to finish Exported 144 of 145 tables.
```

Detectar y reparar datos dañados del programador

Si conoce el nombre de usuario y la contraseña de la base de datos de vCloud Director, utilice el comando `fix-scheduler-data` de la herramienta de administración de celdas para buscar datos dañados del programador en la base de datos 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 5-3. Opciones y argumentos de la herramienta de administración de celdas, subcomando `fix-scheduler-data`

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

Reemplazo de certificados SSL

Utilice el comando `certificates` de la herramienta de administración de celdas para sustituir los certificados SSL de la celda.

El comando `certificates` de la herramienta de administración de celdas automatiza el proceso de sustituir los certificados existentes de una celda por otros almacenados en el almacén de claves JCEKS. El comando `certificates` le permite sustituir certificados de firma automática por certificados firmados. Para crear un almacén de claves JCEKS que contenga certificados firmados, consulte "Creación e importación de certificados SSL firmados," página 19.

Para sustituir los certificados SSL de una celda, utilice un comando con el siguiente formato:

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

Tabla 5-4. Opciones y argumentos de la herramienta de administración de celdas, subcomando `certificates`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--config` (-c)	ruta de acceso completa al archivo `global.properties` de la celda.	De forma predeterminada, es `$VCLOUD_HOME/etc/global.properties`.
`--httpks` (-j)	Ninguno	Genere un archivo de almacén de claves denominado `certificados` para que lo utilice el extremo http.
`--consoleproxyks` (-p)	Ninguno	Genere un archivo de almacén de claves denominado `certificadosproxy` para que lo utilice el extremo proxy de la consola.
`--responses` (-r)	ruta de acceso completa al archivo `responses.properties`	De forma predeterminada, es `$VCLOUD_HOME/etc/responses.properties`.

Tabla 5-4. Opciones y argumentos de la herramienta de administración de celdas, subcomando `certificates` (Continua)

Opción	Argumento	Descripción
`--keystore` (-k)	*almacénClaves-nombreRuta*	Nombre de ruta completo al almacén de claves JCEKS que contiene los certificados firmados. La forma corta y menos recomendada de `-s` ha sido sustituida por `-k`.
`--keystore-password` (-w)	*almacénClaves-contraseña*	Contraseña del almacén de claves JCEKS al que hace referencia la opción `--keystore`. Sustituye a las opciones menos recomendadas de `-kspassword` y `--keystorepwd`.

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
Certificado sustituido por el almacén de claves especificado del usuario en /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.

Generación de certificados SSL de autofirma

Utilice el comando `generate-certs` de la herramienta de administración de celdas para generar certificados SSL de firma automática para la celda.

El comando `generate-certs` de la herramienta de administración de celdas automatiza el procedimiento que se muestra en "Creación de certificados SSL de firma automática," página 22.

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 5-5. Opciones y argumentos de la herramienta de administración de celdas, subcomando `generate-certs`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--expiration` (-x)	*días-hasta-caducidad*	Número de días para que caduquen los certificados. El valor predeterminado es 365.

Tabla 5-5. Opciones y argumentos de la herramienta de administración de celdas, subcomando `generate-certs` (Continua)

Opción	Argumento	Descripción
`--issuer` (-i)	*nombre=valor* [, *nombre=valor*, ...]	Nombre distintivo X.509 del emisor del certificado. El valor predeterminado es `CN=`*FQDN*. donde *FQDN* 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.
`--httpcert` (-j)	Ninguno	Genere un certificado para el extremo HTTP.
`--key-size` (-s)	*tamaño-clave*	Tamaño del par de claves expresado como un número entero de bits. El valor predeterminado es 2048. Observe que los tamaños de clave inferiores a 1024 bits ya no se admiten según la publicación especial NIST 800-131A.
`--keystore-pwd` (-w)	*almacénClaves-contraseña*	Contraseña del almacén de claves de este host.
`--out` (-o)	*almacénClaves-nombreRuta*	Nombre de ruta completo al almacén de claves de este host.
`--consoleproxycert` (-p)	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 4096 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.
```

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 "Ejemplo: Elabore la lista de todos los cifrados permitidos," página 67 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 5-6. 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)	Nombres de cifrados en una lista separada por comas, como se publica en http://www.openssl.org/docs/apps/ciphers.html	No permita los cifrados de la lista separada por comas especificada.

Tabla 5-6. Opciones y argumentos de la herramienta de administración de celdas, subcomando `ciphers` (Continua)

Opción	Argumento	Descripción
`--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 los 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 5-7. Opciones y argumentos de la herramienta de administración de celdas, subcomando `ssl-protocols`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--all-allowed` (-a)	Ninguno	Elabore una lista de todos los protocolos SSL que admite vCloud Director.
`--disallow` (-d)	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.
`--list` (-l)	Ninguno	Elabore una lista de protocolos SSL permitidos que admita la configuración actual de vCloud Director.
`--reset` (-r)	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 **`sl-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 permiten actualmente 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
Protocolos SSL predeterminados del producto: TLSv1.2, TLSv1.1, TLSv1, SSLv3 y 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
Protocolos SSL permitidos: TLSv1.2, TLSv1.1 y TLSv1
```

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`.

Este ejemplo elimina el protocolo SSL TLSv1 de la lista de protocolos SSL permitidos.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool ssl-protocols -d TLSv1, SSLv3 y SSLv2Hello
```

Debe reiniciar la celda después de ejecutar este comando.

Configuración de la conexión de la base de datos de métricas

Utilice el comando `configure-metrics` de la herramienta de administración de celdas para conectar con la 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. Los datos de las métricas históricas se almacenan en una base de datos KairosDB respaldada por Cassandra. Consulte Capítulo 6, "Instalación y configuración de software de bases de datos opcional para almacenar y recuperar las métricas históricas del rendimiento de las máquinas virtuales," página 73.

Para crear una conexión de KairosDB a vCloud Director, utilice una línea de comandos con el siguiente formato:

```
cell-management-tool configure-metrics options
```

Tabla 5-8. Opciones y argumentos de la herramienta de administración de celdas, subcomando `configure-metrics`

Comando	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--repository-host`	Nombre de host o dirección IP del host de KairosDB	Si tiene varias instalaciones de KairosDB, debe proporcionar la dirección del equilibrador de carga aquí.
`--repository-port`	Puerto de KairosDB que se va a usar.	De manera predeterminada, KairosDB utiliza el puerto 8080.

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

En este ejemplo se configura el sistema para que use una instancia de KairosDB alojada en la dirección IP 10.0.0.1 en el puerto predeterminado. La dirección puede ser la de una única máquina en la que se ejecuta una única instancia de KairosDB, o bien la dirección de un equilibrador de carga que distribuye las solicitudes entre varias instalaciones de KairosDB.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]#
./cell-management-tool configure-metrics --repository-host 10.0.0.1 --repository-port 8080
```

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 5-9. Opciones y argumentos de la herramienta de administración de celdas, subcomando `recover-password`

Opción	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--dbuser`	El nombre de usuario de la base de datos de vCloud Director.	Debe proporcionarse en la línea de comandos.
`--dbpassword`	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 las celdas fueron cerradas deliberadamente. No puede utilizar el comando `fail-tasks` hasta que todas las celdas se hayan cerrado.

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 5-10. Opciones y argumentos de la herramienta de administración de celdas, subcomando `fail-tasks`

Comando	Argumento	Descripción
`--help` (-h)	Ninguno	Proporciona un resumen de los comandos disponibles en esta categoría.
`--message` (-m)	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.

Instalación y configuración de software de bases de datos opcional para almacenar y recuperar las métricas históricas del rendimiento de las máquinas virtuales

6

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 una base de datos KairosDB respaldada por un clúster de Cassandra.

Cassandra y KairosDB son bases de datos de código abierto que, cuando se implementan juntas, ofrecen una solución escalable de alto rendimiento para recopilar datos de series temporales como las métricas de máquinas virtuales. Si desea que su nube admita la recuperación de métricas históricas de las máquinas virtuales, debe instalar y configurar Cassandra y KairosDB, y después usar la utilidad `cell-management-tool` para conectar vCloud Director con KairosDB. La recuperación de las métricas actuales no requiere software de base de datos opcional.

Para admitir la recuperación de métricas históricas, vCloud Director requiere un clúster de Cassandra. Un clúster de Cassandra consiste en una o más máquinas en las que se ha instalado Cassandra y están ejecutando el servicio de Cassandra. Para una instalación típica de vCloud Director, deberá tener por lo menos tres máquinas en el clúster de Cassandra. Como la función de supervisión de métricas de vCloud Director utiliza un factor de replicación de dos, tener tres máquinas, los nodos, en el clúster de Cassandra asegura que un nodo siempre está disponible para ocuparse de una transacción. Puede usar un único clúster de Cassandra para la instalación de vCloud Director.

También necesita una instancia de KairosDB, como mínimo, configurada para funcionar con el clúster de Cassandra. Si la nube recopila métricas históricas de muchas máquinas virtuales, se necesitarán más instancias de KairosDB. Puede instalar y configurar KairosDB en uno de los nodos de Cassandra y apuntar la herramienta de gestión de celdas a ese extremo, o bien instalar y configurar KairosDB en cada nodo de Cassandra, agregar un equilibrador de carga al frente de la configuración y apuntar la herramienta de gestión de celdas en el extremo del equilibrador de carga. Como vCloud Director espera comunicarse con KairosDB en una única dirección IP, las instalaciones que incluyen varias instancias de KairosDB deben usar un equilibrador de carga para ofrecer dicha dirección y distribuir las solicitudes de vCloud Director entre las instancias de KairosDB.

Prerequisitos

- Verifique que vCloud Director está instalado y ejecutándose antes de configurar el software de base de datos opcional.
- Si no está familiarizado con Cassandra y KairosDB, revise el material disponible en http://cassandra.apache.org/ y https://code.google.com/p/kairosdb/.
- Obtenga Cassandra 1.2.*x* o Cassandra 2.0.*x* de http://cassandra.apache.org/download/.
- Obtenga KairosDB 0.9.1 de https://code.google.com/p/kairosdb/.
- Complete la instalación y configuración del clúster de Cassandra que piensa utilizar con la instalación de vCloud Director, según esta configuración:
  - Cassandra 1.2.*x* o Cassandra 2.0.*x* está instalado al menos en tres máquinas conectadas a la misma red que las celdas vCloud Director utilizan.

  - Las máquinas están configuradas para disponer de su propio almacenamiento físico, no de almacenamiento compartido.
  - Las máquinas están configuradas como un clúster de Cassandra.
  - Java Native Access (JNA) versión 3.2.7 o posterior está habilitada para el clúster de Cassandra, para mejorar el rendimiento del uso de la memoria y el acceso a disco.
- Complete la instalación y configuración de una instancia de KairosDB 0.9.1 como mínimo en uno de los nodos de Cassandra, para que use el clúster de Cassandra como su base de datos. También puede instalar y configurar KairosDB en cada nodo de Cassandra si agrega un equilibrador de carga al frente de dicha configuración.
- Verifique que KairosDB y Cassandra están correctamente configurados. Utilice un explorador web para ir a `http://KairosDB-IP:8080/api/v1/metricnames`. Si la página se abre sin errores, KairosDB y Cassandra están correctamente configurados.
- Verifique que puede ejecutar el comando `service` de la utilidad `cell-management-tool`. Para obtener detalles sobre el comando `service`, consulte "Inicio o detención de servicios de vCloud Director," página 38.

Procedimiento

1 Use la utilidad `cell-management-tool` para configurar una conexión entre vCloud Director y KairosDB.

  Use un comando como este, donde *KairosDB-IP* es la dirección IP de la máquina en la que instaló KairosDB o la dirección IP del equilibrador de carga que está utilizando para distribuir las solicitudes entre varias instancias de KairosDB.

```
[root@cell1 /opt/vmware/vcloud-
director/bin]# ./cell-management-tool configure-metrics --repository-host KairosDB-IP
--repository-port 8080
```

2 Reinicie cada celda vCloud Director con el comando `service` de la utilidad `cell-management-tool`.

Índice

V