Guía de administración de VMware Integrated OpenStack

VMware Integrated OpenStack 5.1

vmware®

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

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

El sitio web de VMware también ofrece las actualizaciones de producto más recientes.

Si tiene comentarios relacionados con esta documentación, envíelos a:

docfeedback@vmware.com

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

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

Contenido

Guía de administración de VMware Integrated OpenStack

1

En la *Guía de administración de VMware Integrated OpenStack*, se muestra cómo realizar tareas administrativas en VMware Integrated OpenStack, incluido cómo crear y administrar proyectos, usuarios, cuentas, tipos, imágenes y redes.

Público objetivo

Esta guía se orienta a los administradores de nube que desean crear y administrar recursos con una implementación de OpenStack completamente integrada con VMware vSphere®. Para lograr eso correctamente, es necesario estar familiarizado con los componentes y las funciones de OpenStack.

Glosario de publicaciones técnicas de VMware

El departamento de Publicaciones técnicas de VMware ofrece un glosario con los términos que el usuario puede desconocer. Para obtener definiciones de términos tal como se utilizan en la documentación técnica de VMware, visite http://www.vmware.com/support/pubs.

Configuración de implementación 2

Puede modificar la configuración de la implementación de VMware Integrated OpenStack para agregar capacidad, habilitar la generación de perfiles, actualizar las credenciales, y cambiar o personalizar otras opciones.

Este capítulo incluye los siguientes temas:

Agregar capacidad a una implementación de OpenStack

Es posible agregar clústeres de proceso y almacenes de datos a una implementación de VMware Integrated OpenStack existente.

Agregar clústeres de proceso a una implementación de OpenStack

Puede agregar clústeres de proceso a la implementación de VMware Integrated OpenStack para aumentar la capacidad de CPU.

Requisitos previos

En vSphere, cree el clúster que desee agregar a la implementación.

Si desea agregar clústeres de proceso de una instancia de vCenter Server de proceso independiente, se aplican las siguientes restricciones:

- Debe implementar VMware Integrated OpenStack en modo de HA con redes de NSX-T Data Center. Otros modos de implementación y redes no admiten la inclusión de clústeres de proceso de instancias de vCenter Server independientes.
- No es posible agregar clústeres de proceso de instancias de vCenter Server de proceso independientes en la misma zona de disponibilidad.

Procedimiento

1. En vSphere Client, seleccione **Menú > VMware Integrated OpenStack**.
2. Haga clic en **Implementaciones de OpenStack** y abra la pestaña **Administración**.
3. Si desea agregar clústeres de proceso de una instancia de vCenter Server independiente, primero agregue la instancia a la implementación.
   a. Seleccione la pestaña **vCenter Server de procesos**.
   b. Haga clic en el icono **Agregar** (signo más) en la parte superior izquierda del panel.
   c. Introduzca el FQDN de las credenciales de administrador y de la instancia de vCenter Server, y haga clic en **Aceptar**.
4. Seleccione la pestaña **Proceso para Nova**.
5. Haga clic en el icono **Agregar** (signo más) en la parte superior izquierda del panel.
6. Seleccione la zona de disponibilidad y la instancia de vCenter Server del clúster de proceso que desea agregar y haga clic en **Siguiente**.
7. Seleccione el nuevo clúster de proceso y haga clic en **Siguiente**.

   El clúster que se seleccione debe tener al menos un host.
8. Seleccione uno o varios almacenes de datos para que los emplee el clúster de proceso, y haga clic en **Siguiente**.
9. Seleccione la máquina virtual de administración y el almacén de datos deseado y haga clic en **Siguiente**.
10. Revise la configuración propuesta y haga clic en **Finalizar**.

La capacidad de la implementación aumenta junto con el tamaño del clúster de proceso adicional.

Agregar almacenamiento a un nodo informático

Puede aumentar el número de almacenes de datos disponibles para un nodo informático en la implementación de VMware Integrated OpenStack.

La inclusión de un almacén de datos hace que se reinicie el servicio de proceso y puede interrumpir temporalmente los servicios de OpenStack.

Procedimiento

1. En vSphere Client, seleccione **Menú > VMware Integrated OpenStack**.
2. Haga clic en **Implementaciones de OpenStack** y abra la pestaña **Administración**.
3. Abra la pestaña **Nova Storage** y haga clic en el icono **Agregar** (signo más) en la parte superior izquierda del panel.
4. Seleccione el clúster al que desea agregar un almacén de datos y haga clic en **Siguiente**.
5. Seleccione uno o varios almacenes de datos para agregarlos al clúster y haga clic en **Siguiente**.
6. Revise la configuración propuesta y haga clic en **Finalizar**.

La capacidad de almacenamiento del nodo informático seleccionado aumenta junto con el tamaño del almacén de datos adicional.

Agregar almacenamiento a Image Service

Puede aumentar el número de almacenes de datos disponibles para el servicio de imágenes en la implementación de VMware Integrated OpenStack.

La inclusión de un almacén de datos hace que se reinicie el servicio de imágenes y puede interrumpir temporalmente los servicios de OpenStack.

Procedimiento

1. En vSphere Client, seleccione **Menú > VMware Integrated OpenStack**.
2. Haga clic en **Implementaciones de OpenStack** y abra la pestaña **Administración**.
3. Abra la pestaña **Glance Storage** y haga clic en el icono **Agregar** (signo más) en la parte superior izquierda del panel.
4. Seleccione uno o varios almacenes de datos que desee agregar y haga clic en **Siguiente**.
5. Revise la configuración propuesta y haga clic en **Finalizar**.

La capacidad de almacenamiento del servicio de imágenes aumenta junto con el tamaño del almacén de datos adicional.

Agregar nodos al clúster de Swift

Puede agregar nodos de proxy y de almacenamiento para escalar horizontalmente el clúster de Swift.

Importante No se pueden eliminar los nodos en un clúster de Swift. Si desea quitar nodos del clúster, debe eliminar todo el clúster y crearlo de nuevo.

Después de crear un clúster o agregar un nodo de almacenamiento, debe esperar durante una cantidad de tiempo especifica antes de agregar otro nodo de almacenamiento. Este tiempo se establece con el parámetro `--swift-min-part-hours` al crear el clúster. El valor predeterminado es 1 hora.

Si se intenta crear un nodo de almacenamiento antes de que haya transcurrido el tiempo especificado, se producirá un error en la operación y se mostrará el siguiente error en el registro de Ansible: `No se pudieron reasignar particiones. El tiempo entre los procesos de reequilibrio debe ser al menos min_part_hours`.

Requisitos previos

Implemente un clúster de Swift. Consulte "Agregar el componente Swift" en la *Guía de instalación y configuración de VMware Integrated OpenStack*.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Agregue nodos de proxy al clúster.

```
sudo viocli swift add-proxy [--proxy-node-count nodos]
```

Opción	Descripción
--proxy-node-count	Número de nodos de proxy que se agregarán. El valor predeterminado es 1.

3 Agregue nodos de almacenamiento al clúster.

```
sudo viocli swift add-storage --datastores ds1[,ds2...] [--storage-node-count nodes] [--disk-size gb]
```

Opción	Descripción
--datastores	Uno o varios almacenes de datos que los nuevos nodos de almacenamiento de Swift van a utilizar. Separe varias entradas con comas (,).
--storage-node-count	Número de nodos de almacenamiento que se agregarán. El valor predeterminado es 1.
--disk-size	Tamaño de cada disco de almacenamiento en gigabytes. El valor predeterminado es 2048. El disco de almacenamiento de cada nodo creado tendrá el tamaño especificado. Para crear nodos de almacenamiento con discos de diferentes tamaños, debe ejecutar el comando una vez por cada tamaño de disco que desee.

Si lo prefiere, puede preparar las especificaciones deseadas con el formato JSON y ejecutar `sudo viocli swift add-storage -f spec-file.json` para agregar nodos de almacenamiento. Para obtener información sobre el formato requerido, consulte Comando viocli swift.

Agregar intervalos de direcciones IP a una red

Puede agregar rangos de direcciones IP a las redes de la implementación.

Importante Las redes de acceso a la API y de administración no pueden incluir más de 100 direcciones IP cada una.

Procedimiento

1. En vSphere Client, seleccione **Menú > VMware Integrated OpenStack**.
2. Haga clic en **Implementaciones de OpenStack** y abra la pestaña **Administración**.
3. En la pestaña **Redes**, haga clic en el icono **Opciones** (tres puntos) que aparece junto a la red que desea modificar y seleccione **Agregar rango de IP**.
4. Especifique el rango de direcciones IP que desea agregar y haga clic en **Aceptar**.

   Puede hacer clic en **Agregar rango de IP** para agregar varios rangos de direcciones IP a la vez.

Modificar la configuración de DNS de red

Puede modificar la configuración de DNS para las redes de acceso a la API y de administración.

Importante Si se modifica la configuración de DNS de red, se interrumpirá brevemente la conexión de red.

Procedimiento

1. En vSphere Client, seleccione **Menú > VMware Integrated OpenStack**.
2. Haga clic en **Implementaciones de OpenStack** y abra la pestaña **Administración**.
3. En la pestaña **Redes**, haga clic en el icono **Opciones** (tres puntos) que aparece junto a la red que desea modificar y seleccione **Cambiar DNS**.
4. Especifique la dirección IP de los servidores DNS principales y secundarios, y haga clic en **Aceptar**.

Actualizar credenciales de componentes

La implementación de VMware Integrated OpenStack incluye credenciales con las que OpenStack puede acceder y conectarse al servidor LDAP, NSX Manager y la instancia de vCenter Server. Es posible modificar estas credenciales en la vApp de VMware Integrated OpenStack.

Importante Si desea cambiar la contraseña de NSX-T Data Center, realice los siguientes pasos:

1. Inicie sesión en un nodo de controlador y ejecute el comando `systemctl stop neutron-server` para detener el servicio del servidor Neutron.
2. Cambie la contraseña en NSX-T Data Center.
3. Cambie la contraseña en VMware Integrated OpenStack tal como se describe en la siguiente sección.

El servicio del servidor Neutron se reiniciará después de cambiar la contraseña en VMware Integrated OpenStack.

Procedimiento

1. En vSphere Client, seleccione **Menú > VMware Integrated OpenStack**.

2 Haga clic en **Implementaciones de OpenStack** y abra la pestaña **Administración**.

3 En la pestaña **Configuración**, haga clic en **Cambiar contraseña**.

El panel **Cambiar contraseñas** contiene cuadros de texto para actualizar las credenciales actuales del servidor LDAP, NSX Manager y vCenter Server.

4 Introduzca las credenciales actualizadas y haga clic en **Enviar**.

Para conservar la configuración original de un componente, deje en blanco los cuadros de texto.

Agregar certificados a la implementación

Puede agregar certificados digitales a la implementación en la vApp de VMware Integrated OpenStack.

Una entidad de certificación (Certificate Authority, CA) debe firmar los certificados que agregue y estos deben crearse a partir de una solicitud de firma del certificado (Certificate Signing Request, CSR) que VMware Integrated OpenStack genera. No se admite el uso de certificados comodín.

Procedimiento

1 En vSphere Client, seleccione **Menú > VMware Integrated OpenStack**.

2 Haga clic en **Implementaciones de OpenStack** y abra la pestaña **Administración**.

3 En la pestaña **Configuración**, seleccione **Certificado SSL de OpenStack**.

4 Si se requiere un nuevo certificado firmado por una CA, introduzca la información de la CSR y haga clic en **Generar**.

5 Después de obtener el certificado de la CA, haga clic en **Importar** y seleccione el archivo de certificado.

El certificado se agrega a la implementación.

Configurar la limitación de frecuencia de la API pública

Al limitar la frecuencia de llamadas realizadas a los servicios de la API, las operaciones serán más confiables y se reducirá la incidencia de objetos huérfanos durante cargas altas.

Si un cliente supera el límite de frecuencia, recibe una respuesta HTTP `429: Demasiadas solicitudes`. El encabezado `Retry–After` de la respuesta indica cuánto tiempo debe esperar el cliente antes de realizar más llamadas.

Puede habilitar la limitación de frecuencia por servicio. Por ejemplo, es posible que desee limitar las llamadas al servicio de API de Nova de una forma más estricta que las llamadas al servicio de API de Neutron.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

3 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

4 Quite la marca de comentario del parámetro `haproxy_throttle_period` y establézcalo como el número de segundos que deben esperar los clientes si se supera un límite de frecuencia.

5 Si desea configurar límites de frecuencia para API específicas, quite la marca de comentario de los parámetros `max_requests` y `request_period` para dichos servicios y configúrelos como desee.

A continuación se enumeran las API cuya frecuencia puede limitarse y los parámetros correspondientes.

Opción	Descripción
haproxy_keystone_max_requests **haproxy_keystone_request_period**	API de Keystone
haproxy_keystone_admin_max_requests **haproxy_keystone_admin_request_period**	API del administrador de Keystone
haproxy_glance_max_requests **haproxy_glance_request_period**	API de Glance
haproxy_nova_max_requests **haproxy_nova_request_period**	API de Nova
haproxy_nova_placement_max_requests **haproxy_nova_placement_request_period**	API de colocación de Nova
haproxy_cinder_max_requests **haproxy_cinder_request_period**	API de Cinder
haproxy_designate_max_requests **haproxy_designate_request_period**	API de Designate
haproxy_neutron_max_requests **haproxy_neutron_request_period**	API de Neutron
haproxy_heat_max_requests **haproxy_heat_request_period**	API de Heat
haproxy_heat_cfn_max_requests **haproxy_heat_cfn_request_period**	API de Heat CloudFormation
haproxy_heat_cloudwatch_max_requests **haproxy_heat_cloudwatch_request_period**	API de Heat CloudWatch

Opción	Descripción
haproxy_ceilometer_max_requests **haproxy_ceilometer_request_period**	API de Ceilometer
haproxy_aodh_max_requests **haproxy_aodh_request_period**	API de Aodh
haproxy_panko_max_requests **haproxy_panko_request_period**	API de Panko

6 Implemente la configuración actualizada.

```
sudo viocli deployment configure ––limit lb
```

Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

Ejemplo: Limitar las llamadas a la API pública de Neutron

La siguiente configuración limita las llamadas a la API pública de Neutron. Si una única dirección IP de origen envía más de 50 solicitudes a la API pública de Neutron en un periodo de 10 segundos, los equilibradores de carga devolverán errores HTTP 429 a todas las solicitudes posteriores realizadas desde esa dirección de origen durante un período de 60 segundos. Transcurridos 60 segundos, la dirección de origen puede reanudar el envío de solicitudes a la API pública de Neutron.

```
haproxy_throttle_period: 60
haproxy_neutron_max_requests: 50
haproxy_neutron_request_period: 10
```

Modificar la configuración de cifrado en ejecución

Puede cambiar los conjuntos de claves de cifrado que HAProxy utiliza y especificar si desea cifrar los datos en ejecución que se transfieren entre endpoints internos.

Todos los endpoints de API públicos en una implementación de VMware Integrated OpenStack utilizan el cifrado de TLS 1.2. Para las implementaciones de HA, el tráfico entre endpoints internos también se cifra mediante TLS. Debido a que los endpoints internos de una implementación compacta o muy pequeña se encuentran en una sola máquina virtual, el tráfico entre los endpoints internos no se cifra para esos tipos de implementación de forma predeterminada.

Cuando se habilita el cifrado en ejecución interno, HAProxy actúa como un equilibrador de carga de capa 4 en lugar de uno de capa 7 para las llamadas a API internas y el tráfico de Horizon. Para garantizar el rendimiento del cifrado de alta seguridad, el servidor HTTP Apache de cada controlador finaliza TLS para cada servicio de OpenStack individual. A continuación, el servidor Apache reenvía la solicitud a través de un servicio de bucle invertido local al servicio de back-end (como Nova, Neutron o Cinder). HAProxy también vuelve a cifrar la solicitud cuando la envía a un nodo de controlador de back-end a través de la red interna.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

3. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
4. Modifique la configuración de cifrado según desee.
   - Para ajustar los conjuntos de claves de cifrado, quite la marca de comentario del parámetro `haproxy_ssl_default_bind_ciphers` y establezca su valor como el conjunto de claves de cifrado que desee.
   - Para activar o desactivar la protección de TLS para los endpoints internos, quite la marca de comentario del parámetro `internal_api_protocol` y establezca su valor como **`https`** (TLS habilitado) o **`http`** (TLS deshabilitado).
5. Implemente la configuración actualizada.

   ```
   sudo viocli deployment configure
   ```

   Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.
6. Si cambia el valor del parámetro `internal_api_protocol`, actualice la URL del endpoint de Keystone según corresponda.
   a. En vSphere Web Client, seleccione **Administración > OpenStack**.

   Nota Actualmente, vSphere Client HTML5 no admite esta operación. Utilice la instancia de vSphere Web Client basada en Flex.

   b. Seleccione el endpoint de **KEYSTONE** y haga clic en el icono de **edición** (lápiz).

   c. En la sección **Actualizar endpoint**, cambie la dirección URL para que comience con `http` o `https` en función de la configuración.

   d. Introduzca la contraseña del administrador y haga clic en **Actualizar**.

Personalizar logotipos de Horizon

Puede personalizar los logotipos que aparecen en la página de inicio de sesión del panel de control de VMware Integrated OpenStack y en la esquina superior izquierda de otras páginas.

De forma predeterminada, el logotipo corporativo de VMware se utiliza en la página de inicio de sesión y en la esquina superior izquierda de cada página en el panel de control. Puede cargar un archivo de gráfico personalizado en Servidor de administración de OpenStack y configurarlo para que se muestre como el logotipo de inicio de sesión o del panel de control.

Requisitos previos

- Los logotipos personalizados deben tener 216 píxeles de largo por 35 píxeles de ancho. Puede que gráficos con dimensiones diferentes no se muestren correctamente.
- Los archivos de logotipo personalizado deben tener el formato SVG o PNG.

Procedimiento

1. Use SCP para transferir los archivos de logotipo personalizado a un directorio temporal en la máquina virtual de Servidor de administración de OpenStack como la cuenta `viouser`.

   ```
   scp your-logo-file viouser@mgmt-server-ip:/home/viouser/
   ```

2. Inicie sesión en la máquina virtual de Servidor de administración de OpenStack como la cuenta `viouser`.

   ```
   ssh viouser@mgmt-server-ip
   ```

3. Cree el directorio `/opt/vmware/vio/custom/horizon` y mueva el archivo de logotipo a ese directorio.

   ```
   sudo mkdir -p /opt/vmware/vio/custom/horizon
   sudo mv /home/viouser/your-logo-file /opt/vmware/vio/custom/horizon/
   ```

4. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

5. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
   - Para configurar un logotipo de inicio de sesión, modifique el parámetro siguiente:

     ```
     #horizon_logo_splash: "/opt/vmware/vio/custom/horizon/logo_file"
     ```

   - Para configurar un logotipo de panel de control, modifique el parámetro siguiente:

     ```
     #horizon_logo: "/opt/vmware/vio/custom/horizon/logo_file"
     ```

6. Elimine el signo de número (#) para quitar la marca de comentario del parámetro que desea habilitar. A continuación, reemplace `logo_file` por el nombre del archivo de gráfico personalizado.

   ```
   horizon_logo_splash: "/opt/vmware/vio/custom/horizon/your-login-logo"
   horizon_logo: "/opt/vmware/vio/custom/horizon/your-dash-logo"
   ```

   Puede habilitar uno o ambos parámetros.

7 Implemente la configuración actualizada.

```
sudo viocli deployment configure --tags horizon
```

Crear perfiles de servicios de OpenStack

Puede utilizar OSProfiler para habilitar el seguimiento de los servicios básicos de la implementación de OpenStack. El seguimiento captura el tiempo de respuesta de todas las llamadas API, RPC, de controladores y de base de datos que forman parte de una operación de OpenStack.

VMware Integrated OpenStack admite la creación de perfiles de los comandos Cinder, Glance, Heat, Neutron y Nova. Puede almacenar datos de seguimiento del generador de perfiles con Ceilometer o vRealize Log Insight.

Requisitos previos

- Si desea utilizar Ceilometer para almacenar datos de seguimiento, habilite Ceilometer. Consulte "Habilitar el componente Ceilometer" en la *Guía de instalación y configuración de VMware Integrated OpenStack*.
- Si desea utilizar vRealize Log Insight para almacenar datos de seguimiento, implemente y configure vRealize Log Insight. Consulte el documento *Introducción* para vRealize Log Insight.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

```
sudo mkdir -p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

3 Quite la marca de comentario del parámetro `os_profiler_enabled` y establezca su valor como **`true`**.

4 Quite el comentario del parámetro `os_profiler_hmac_keys` e introduzca una contraseña para OSProfiler.

5 Si utiliza vRealize Log Insight, quite el comentario del parámetro `os_profiler_connection_string` y establezca su valor en la ubicación del servidor vRealize Log Insight.

   Introduzca la dirección del servidor vRealize Log Insight con el siguiente formato: "`loginsight://`*`username`*`:`*`password`*`@`*`loginsight-ip`*"

   Especifique el nombre de usuario y la contraseña de un usuario con la función `USER` en la implementación de vRealize Log Insight.

6 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

7 Si utiliza vRealize Log Insight, inicie sesión en el nodo de controlador y establezca la variable de entorno `OSPROFILER_CONNECTION_STRING` en la dirección del servidor vRealize Log Insight que utilizó en el paso 5.

```
export OSPROFILER_CONNECTION_STRING="loginsight://username:password@loginsight-ip"
```

Ahora puede habilitar la generación de perfiles en los comandos de OpenStack. Ejecute el comando que desee con el parámetro `--profile` y especifique la contraseña de OSProfiler. El comando genera un UUID de seguimiento de generación de perfiles. Ejecute OSProfiler con ese UUID para generar un informe. Por ejemplo:

```
cinder list --profile osprofiler-password
osprofiler trace show --html profiling-uuid
```

Instancias de OpenStack en vSphere

Las instancias que se crean en la implementación de VMware Integrated OpenStack aparecen como máquinas virtuales en el inventario de vCenter Server. Se aplican numerosas restricciones a la forma de administrar máquinas virtuales de OpenStack y trabajar con esas máquinas.

En la mayoría de los casos, debe administrar las máquinas virtuales de OpenStack en la CLI o el panel de control de VMware Integrated OpenStack en lugar de en vSphere Client.

Funciones de OpenStack compatibles con vSphere

vSphere admite ciertas funciones de OpenStack.

Función de OpenStack	Compatible con vSphere
Iniciar	SÍ
Reiniciar	SÍ
Finalizar	SÍ
Cambiar de tamaño	SÍ
Recuperar	SÍ
Pausar	NO
Anular pausa	NO
Suspender	SÍ
Reanudar	SÍ

Función de OpenStack	Compatible con vSphere
Insertar redes Esta función solo se admite cuando se presentan las siguientes condiciones: ■ Con la red Nova en modo Flat ■ Con máquinas virtuales basadas en Debian o Ubuntu ■ En el tiempo de arranque	SÍ
Insertar archivo	NO
Salida de consola serie	SÍ
Consola RDP	NO
Asociar volumen	SÍ
Desasociar volumen	SÍ
Migración en vivo	SÍ
Instantánea	SÍ
iSCSI	SÍ
Canal de fibra	SÍ Compatible en los almacenes de datos de vSphere
Establecer contraseña de administrador	NO
Obtener información de invitado	SÍ
Establecer información de host	SÍ
Integración con Glance	SÍ
Control de servicios	SÍ
Redes VLAN	SÍ
Redes Flat	SÍ
Grupos de seguridad	NO vSphere Client es compatible con grupos de seguridad cuando se usa el complemento Neutron de NSX Data Center for vSphere.
Reglas de firewall	NO
Enrutamiento	SÍ
Unidad de configuración	SÍ
Modo de evaluación o de mantenimiento de host	SÍ
Intercambio de volúmenes	NO
Límite de tasa de volúmenes	NO

Operaciones con máquinas virtuales en OpenStack

En la siguiente tabla se detallan las operaciones con máquinas virtuales de VMware Integrated OpenStack y vSphere, y se recomienda la ubicación ideal para ejecutar cada operación. Si crea una máquina virtual en VMware Integrated OpenStack, administre esa máquina en VMware Integrated OpenStack.

Función de vSphere	Equivalente en OpenStack	Se expone mediante la API de OpenStack	Ubicación para ejecutar esta operación
Crear una máquina virtual	Iniciar instancia	SÍ	Panel de control de OpenStack
Reiniciar	Reiniciar	SÍ	Panel de control de OpenStack o vSphere Client
Eliminar	Finalizar	SÍ	Panel de control de OpenStack
Cambiar de tamaño	Cambiar de tamaño	SÍ	Panel de control de OpenStack
Pausar	Pausar	SÍ	Panel de control de OpenStack o vSphere Client
Anular pausa	Anular pausa	SÍ	OpenStack o vSphere Client
Pausar	Suspender	SÍ	Panel de control de OpenStack
Reanudar	Reanudar	SÍ	Panel de control de OpenStack
Salida de consola serie	Salida de consola serie	SÍ	Panel de control de OpenStack o vSphere Client
Consola RDP	Consola RDP		Panel de control de OpenStack o vSphere Client
Agregar disco	Asociar volumen	SÍ	Panel de control de OpenStack
Eliminar disco	Desasociar volumen	SÍ	Panel de control de OpenStack
vMotion	Migración en vivo	SÍ	vSphere Client
Instantánea	Instantánea	SÍ	Panel de control de OpenStack o vSphere Client
Funciones disponibles a través de VMware Tools.	Obtener información de invitado/host	SÍ	Panel de control de OpenStack o vSphere Client Para vSphere Client, esta función se encuentra disponible con VMware Tools.
Grupos de puertos distribuidos	Redes VLAN o Flat	SÍ	Panel de control de OpenStack
Función disponible a través de VMware Tools.	Unidad de configuración	NO	Panel de control de OpenStack o vSphere Client Para vSphere Client, esta función se encuentra disponible con VMware Tools.
Instalar VMware Tools en una máquina virtual	Instalar VMware Tools en una máquina virtual	NO	Panel de control de OpenStack o vSphere Client

Funciones de vCenter Server no compatibles con la API de OpenStack

No existe paridad directa entre las funciones de OpenStack y las funciones de vSphere. La API de OpenStack no admite las siguientes funciones de vCenter Server.

- Agregar un host a un clúster

  OpenStack no puede agregar un host a un clúster en vSphere.

- Colocar un host en modo de mantenimiento

  Un host se coloca en modo de mantenimiento por cuestiones de soporte, por ejemplo, para instalar más memoria. Un host ingresa al modo de mantenimiento o sale de ese modo únicamente por solicitud del usuario. No existe una función así en OpenStack. Consulte la documentación de vSphere para obtener instrucciones sobre la forma de ingresar y salir del modo de mantenimiento.

- Grupos de recursos

  En vSphere, un grupo de recursos es una abstracción lógica para administrar de forma flexible los recursos, como la CPU y la memoria. OpenStack no posee un equivalente para el grupo de recursos.

- Instantáneas de vSphere

  vCenter Server admite las instantáneas de OpenStack, pero las instantáneas de vSphere son diferentes y no son compatibles con la API de OpenStack.

Crear un centro de datos virtual de arrendatario

Puede crear centros de datos virtuales de tenant para habilitar la asignación de recursos y de varios tenants segura. Estos centros de datos pueden crearse en nodos informáticos diferentes que ofrecen acuerdos de nivel de servicio específicos para cada carga de trabajo de telecomunicaciones.

Importante Esta función solo está disponible en VMware Integrated OpenStack Carrier Edition. Para obtener más información, consulte "Licencias de VMware Integrated OpenStack" en la *Guía de instalación y configuración de VMware Integrated OpenStack*.

Las cuotas de proyecto limitan los recursos de OpenStack en varios nodos informáticos o zonas de disponibilidad, pero no garantizan la disponibilidad de los recursos. Al crear un centro de datos virtual de tenant para asignar CPU y memoria a un proyecto de OpenStack en un nodo informático, se garantizan los recursos para los tenants y se evitan escenarios de tenants que monopolizan recursos en un entorno de varios tenants.

El centro de datos virtual de tenant asigna recursos a nivel de nodo informático. También puede asignar recursos a nivel de función de red virtual (Virtual Network Function, VNF) con el mismo tipo. Para obtener instrucciones, consulte Configurar la asignación de recursos de QoS para instancias mediante metadatos de tipo.

Puede administrar centros de datos virtuales de tenant mediante la utilidad `viocli`, las vAPI o Data Center Command-Line Interface (DCLI). Este procedimiento emplea la utilidad `viocli` como ejemplo. Para obtener información sobre el uso de la vAPI o DCLI, consulte Usar las vAPI del centro de datos virtual de tenant.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Cree un centro de datos virtual de tenant.

```
viocli inventory-admin create-tenant-vdc --project-id project-uuid --compute compute-node --name
display-name [--cpu-limit max-cpu-mhz] [--cpu-reserve min-cpu-mhz] [--mem-limit max-memory-mb] [--
mem-reserve min-memory-mb]
```

3 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

4 En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.

5 Configure un tipo para utilizar el centro de datos virtual de tenant.

   a Seleccione **Administrador > Proceso > Tipos**.

   b Cree un nuevo tipo o elija uno existente para utilizarlo para el acceso directo.

   c Seleccione la opción **Actualizar metadatos** que aparece junto al tipo que desea utilizar.

   d En el panel **Metadatos disponibles**, expanda **Directivas de VMware** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Centro de datos virtual de tenant**.

   e Establezca el valor de `vmware:tenant_vdc` como el UUID del centro de datos virtual de tenant y haga clic en **Guardar**.

      Puede ejecutar el comando `viocli inventory-admin list-tenant-vdcs` en Servidor de administración de OpenStack para buscar el UUID de todos los centros de datos virtuales de tenant.

Se crea el centro de datos virtual de tenant. Ahora puede iniciar instancias en el centro de datos virtual de tenant configurándolas con el tipo que modificó en este procedimiento.

Pasos siguientes

Puede mostrar los grupos de recursos en un centro de datos virtual de tenant ejecutando el comando `viocli inventory-admin show-tenant-vdc --id tvdc-uuid`. Cada grupo de recursos se muestra con su identificador de proveedor, identificador de proyecto, estado, CPU máxima y mínima, memoria máxima y mínima, e información del nodo informático. Si un centro de datos virtual de tenant incluye varios grupos de recursos, la primera fila muestra información agregada de todos los grupos.

Puede actualizar los centros de datos virtuales de tenant ejecutando el comando `viocli inventory-admin update-tenant-vdc`. Para obtener parámetros específicos, consulte Comando viocli inventory-admin.

Puede eliminar un centro de datos virtual de tenant que no necesite ejecutando el comando `viocli inventory-admin delete-tenant-vdc --id tvdc-uuid`.

Configuración de red de Neutron 3

Puede crear redes externas y del proveedor para la implementación de VMware Integrated OpenStack, configurar zonas de disponibilidad y realizar otras tareas de redes avanzadas.

Este capítulo incluye los siguientes temas:

Crear una red del proveedor

Las redes del proveedor se asignan a redes físicas en el centro de datos y sus funciones de redes las realizan dispositivos físicos.

Una red del proveedor se puede dedicar a un proyecto o compartirse entre varios proyectos. Los tenants pueden crear máquinas virtuales en redes del proveedor o conectar sus redes de tenant a una red del proveedor a través de un enrutador de Neutron.

La configuración específica para crear una red del proveedor depende del modo de redes de la implementación de VMware Integrated OpenStack.

Crear una red de proveedor con NSX-T Data Center

Con las redes de NSX-T Data Center, puede crear una red del proveedor basada en VLAN.

Requisitos previos

Defina una VLAN para la red del proveedor y registre su identificador.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.

3 Seleccione **Administrador > Red > Redes**.

4 Haga clic en **Crear red** y configure la red del proveedor.

Opción	Descripción
Nombre	Introduzca un nombre para la red.
Proyecto	Seleccione el proyecto que desee del menú desplegable.
Tipo de red del proveedor	Seleccione **VLAN** en el menú desplegable.
Red física	Introduzca el UUID de la zona de transporte de VLAN.
ID de segmentación	Introduzca el identificador de VLAN definido para la red del proveedor.

5 Seleccione **Habilitar estado de administrador** y **Crear subred**.

6 Si desea que varios proyectos utilicen la red del proveedor, seleccione **Compartida**.

7 Haga clic en **Siguiente** y configure la subred.

Opción	Descripción
Nombre de la subred	Introduzca un nombre para la subred.
Dirección de red	Introduzca el rango de direcciones IP para la subred en formato CIDR (por ejemplo, 192.0.2.0/24).
Versión de IP	Seleccione **IPv4** o **IPv6**.
IP de puerta de enlace	Introduzca la dirección IP de puerta de enlace. Si no introduce ningún valor, se utilizará la primera dirección IP de la subred. Si no desea una puerta de enlace en la subred, seleccione **Deshabilitar puerta de enlace**.

8 (opcional) Configure opciones adicionales para la subred.

   a En **Grupos de asignación**, introduzca los grupos de direcciones IP a partir de los que se asignarán las direcciones IP de las máquinas virtuales creadas en la red. Introduzca los grupos como dos direcciones IP separadas un coma (por ejemplo, **`192.0.2.10,192.0.2.15`**). Si no especifica ningún grupo de direcciones IP, la subred completa estará disponible para su asignación.

   b En **Servidores de nombres DNS**, introduzca la dirección IP de uno o varios servidores DNS que se usarán en la subred.

   c En **Rutas de host**, introduzca rutas adicionales para anunciar los hosts en la subred. Introduzca las rutas como la dirección IP de destino en formato CIDR y el próximo salto separados por una coma (por ejemplo, **`192.0.2.0/24,192.51.100.1`**).

9 Haga clic en **Crear**.

Crear una red de proveedor con NSX Data Center for vSphere

Con redes de NSX Data Center for vSphere, puede crear una red del proveedor sin formato, basada en VLAN, basada en grupo de puertos o basada en VXLAN.

Requisitos previos

- Si desea crear una red basada en VLAN, defina una VLAN para la red del proveedor y registre su identificador.
- Si desea crear una red basada en grupos de puertos, cree un grupo de puertos para la red del proveedor y registre su identificador de objeto administrado (Managed Object Identifier, MOID).

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.
2. En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.
3. Seleccione **Administrador > Red > Redes**.
4. Haga clic en **Crear red** y configure la red del proveedor.

Opción	Descripción
Nombre	Introduzca un nombre para la red.
Proyecto	Seleccione el proyecto que desee del menú desplegable.
Tipo de red del proveedor	Seleccione **Sin formato**, **VLAN**, **Grupo de puertos** o **VXLAN** del menú desplegable.
Red física	■ Si seleccionó **Sin formato** o **VLAN** para el tipo de red, introduzca el MOID del conmutador distribuido para la red del proveedor. ■ Si seleccionó **Grupo de puertos** para el tipo de red, introduzca el MOID del grupo de puertos para la red del proveedor. ■ Si seleccionó **VXLAN** para el tipo de red, este valor se determina automáticamente.
ID de segmentación	Si seleccionó **VLAN** para el tipo de red, introduzca el identificador de VLAN definido para la red del proveedor.

5. Seleccione **Habilitar estado de administrador** y **Crear subred**.
6. Si desea que varios proyectos utilicen la red del proveedor, seleccione **Compartida**.
7. Haga clic en **Siguiente** y configure la subred.

Opción	Descripción
Nombre de la subred	Introduzca un nombre para la subred.
Dirección de red	Introduzca el rango de direcciones IP para la subred en formato CIDR (por ejemplo, 192.0.2.0/24).

Opción	Descripción
Versión de IP	Seleccione **IPv4** o **IPv6**.
IP de puerta de enlace	Introduzca la dirección IP de puerta de enlace. Si no introduce ningún valor, se utilizará la primera dirección IP de la subred. Si no desea una puerta de enlace en la subred, seleccione **Deshabilitar puerta de enlace**.

8 (opcional) Configure opciones adicionales para la subred.

a En **Grupos de asignación**, introduzca los grupos de direcciones IP a partir de los que se asignarán las direcciones IP de las máquinas virtuales creadas en la red. Introduzca los grupos como dos direcciones IP separadas un coma (por ejemplo, **`192.0.2.10,192.0.2.15`**). Si no especifica ningún grupo de direcciones IP, la subred completa estará disponible para su asignación.

b En **Servidores de nombres DNS**, introduzca la dirección IP de uno o varios servidores DNS que se usarán en la subred.

c En **Rutas de host**, introduzca rutas adicionales para anunciar los hosts en la subred. Introduzca las rutas como la dirección IP de destino en formato CIDR y el próximo salto separados por una coma (por ejemplo, **`192.0.2.0/24,192.51.100.1`**).

9 Haga clic en **Crear**.

Crear una red del proveedor con redes de VDS

Con las redes de VDS, puede crear una red del proveedor basada en VLAN.

Requisitos previos

Defina una VLAN para la red del proveedor y registre su identificador.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.

3 Seleccione **Administrador > Red > Redes**.

4 Haga clic en **Crear red** y configure la red del proveedor.

Opción	Descripción
Nombre	Introduzca un nombre para la red.
Proyecto	Seleccione el proyecto que desee del menú desplegable.
Tipo de red del proveedor	Seleccione **VLAN** en el menú desplegable.
Red física	Introduzca **dvs**.
ID de segmentación	Introduzca el identificador de VLAN definido para la red del proveedor.

5 Seleccione **Habilitar estado de administrador** y **Crear subred**.

6 Si desea que varios proyectos utilicen la red del proveedor, seleccione **Compartida**.

7 Haga clic en **Siguiente** y configure la subred.

Opción	Descripción
Nombre de la subred	Introduzca un nombre para la subred.
Dirección de red	Introduzca el rango de direcciones IP para la subred en formato CIDR (por ejemplo, 192.0.2.0/24).
Versión de IP	Seleccione **IPv4** o **IPv6**.
IP de puerta de enlace	Introduzca la dirección IP de puerta de enlace. Si no introduce ningún valor, se utilizará la primera dirección IP de la subred. Si no desea una puerta de enlace en la subred, seleccione **Deshabilitar puerta de enlace**.

8 (opcional) Configure opciones adicionales para la subred.

a En **Grupos de asignación**, introduzca los grupos de direcciones IP a partir de los que se asignarán las direcciones IP de las máquinas virtuales creadas en la red. Introduzca los grupos como dos direcciones IP separadas un coma (por ejemplo, **`192.0.2.10,192.0.2.15`**). Si no especifica ningún grupo de direcciones IP, la subred completa estará disponible para su asignación.

b En **Servidores de nombres DNS**, introduzca la dirección IP de uno o varios servidores DNS que se usarán en la subred.

c En **Rutas de host**, introduzca rutas adicionales para anunciar los hosts en la subred. Introduzca las rutas como la dirección IP de destino en formato CIDR y el próximo salto separados por una coma (por ejemplo, **`192.0.2.0/24,192.51.100.1`**).

9 Haga clic en **Crear**.

Crear una red externa

Las redes externas actúan como grupos de direcciones IP flotantes para proporcionar acceso externo a las instancias de la implementación.

Una red externa se puede dedicar a un proyecto o compartirse entre varios proyectos. Los tenants no pueden crear máquinas virtuales en redes externas.

La configuración específica para crear una red externa depende del modo de redes de la implementación de VMware Integrated OpenStack.

Crear una red externa con NSX-T Data Center

Para las implementaciones de NSX-T Data Center, se crea una red externa en la que se encuentran las direcciones IP flotantes de los enrutadores (nivel 1) lógicos de tenant futuros.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.

3 Seleccione **Administrador > Red > Redes**.

4 Haga clic en **Crear red** y configure la red del proveedor.

Opción	Descripción
Nombre	Introduzca un nombre para la red.
Proyecto	Seleccione el proyecto que desee del menú desplegable.
Tipo de red del proveedor	Seleccione **Local** para conectar los enrutadores lógicos de tenant con el enrutador de nivel 0 predeterminado, o **Externa** para conectar los enrutadores lógicos de tenant con otro enrutador de nivel 0.
Red física	Si seleccionó **Externa** como tipo de red del proveedor, especifique el UUID del enrutador de nivel 0 al que desee conectar los enrutadores lógicos de tenant futuros.

5 Seleccione **Habilitar estado de administrador**, **Red externa** y **Crear subred**.

6 Si desea que varios proyectos utilicen la red externa, seleccione **Compartida**.

7 Haga clic en **Siguiente** y configure la subred.

Opción	Descripción
Nombre de la subred	Introduzca un nombre para la subred.
Dirección de red	Introduzca el rango de direcciones IP para la subred en formato CIDR (por ejemplo, 192.0.2.0/24).
Versión de IP	Seleccione **IPv4** o **IPv6**.
IP de puerta de enlace	Introduzca la dirección IP de puerta de enlace. Si no introduce ningún valor, se utilizará la primera dirección IP de la subred. Si no desea una puerta de enlace en la subred, seleccione **Deshabilitar puerta de enlace**.

8 Haga clic en **Siguiente** y anule la selección de **Habilitar DHCP**.

9 (opcional) Configure opciones adicionales para la subred.

a En **Grupos de asignación**, introduzca grupos de direcciones IP a partir de los que asignará las direcciones IP flotantes de los enrutadores lógicos de tenant. Introduzca los grupos como dos direcciones IP separadas un coma (por ejemplo, **`192.0.2.10,192.0.2.15`**). Si no especifica ningún grupo de direcciones IP, la subred completa estará disponible para su asignación.

b En **Servidores de nombres DNS**, introduzca la dirección IP de uno o varios servidores DNS que se usarán en la subred.

c En **Rutas de host**, introduzca rutas adicionales para anunciar los hosts en la subred. Introduzca las rutas como la dirección IP de destino en formato CIDR y el próximo salto separados por una coma (por ejemplo, **`192.0.2.0/24,192.51.100.1`**).

10 Haga clic en **Crear**.

Crear una red externa con NSX Data Center for vSphere

Con redes de NSX Data Center for vSphere, puede crear una red externa sin formato, basada en VLAN, basada en grupo de puertos o basada en VXLAN.

Requisitos previos

- Si desea crear una red basada en VLAN, defina una VLAN para la red externa y registre su identificador.
- Si desea crear una red basada en grupos de puertos, cree un grupo de puertos para la red externa y registre su identificador de objeto administrado (Managed Object Identifier, MOID).

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.
2. En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.
3. Seleccione **Administrador > Red > Redes**.
4. Haga clic en **Crear red** y configure la red del proveedor.

Opción	Descripción
Nombre	Introduzca un nombre para la red.
Proyecto	Seleccione el proyecto que desee del menú desplegable.
Tipo de red del proveedor	Seleccione **Sin formato**, **VLAN**, **Grupo de puertos** o **VXLAN** del menú desplegable.
Red física	■ Si seleccionó **Sin formato** o **VLAN** para el tipo de red, introduzca el MOID del conmutador distribuido para la red del proveedor. ■ Si seleccionó **Grupo de puertos** para el tipo de red, introduzca el MOID del grupo de puertos para la red del proveedor. ■ Si seleccionó **VXLAN** para el tipo de red, este valor se determina automáticamente.
ID de segmentación	Si seleccionó **VLAN** para el tipo de red, introduzca el identificador de VLAN definido para la red del proveedor.

5. Seleccione **Habilitar estado de administrador**, **Red externa** y **Crear subred**.
6. Si desea que varios proyectos utilicen la red del proveedor, seleccione **Compartida**.
7. Haga clic en **Siguiente** y configure la subred.

Opción	Descripción
Nombre de la subred	Introduzca un nombre para la subred.
Dirección de red	Introduzca el rango de direcciones IP para la subred en formato CIDR (por ejemplo, 192.0.2.0/24).
Versión de IP	Seleccione **IPv4** o **IPv6**.
IP de puerta de enlace	Introduzca la dirección IP de puerta de enlace. Si no introduce ningún valor, se utilizará la primera dirección IP de la subred. Si no desea una puerta de enlace en la subred, seleccione **Deshabilitar puerta de enlace**.

8. Haga clic en **Siguiente** y anule la selección de **Habilitar DHCP**.

9 (opcional) Configure opciones adicionales para la subred.

   a En **Grupos de asignación**, introduzca grupos de direcciones IP a partir de los que asignará las direcciones IP flotantes de los enrutadores lógicos de tenant. Introduzca los grupos como dos direcciones IP separadas un coma (por ejemplo, **`192.0.2.10,192.0.2.15`**). Si no especifica ningún grupo de direcciones IP, la subred completa estará disponible para su asignación.

   b En **Servidores de nombres DNS**, introduzca la dirección IP de uno o varios servidores DNS que se usarán en la subred.

   c En **Rutas de host**, introduzca rutas adicionales para anunciar los hosts en la subred. Introduzca las rutas como la dirección IP de destino en formato CIDR y el próximo salto separados por una coma (por ejemplo, **`192.0.2.0/24,192.51.100.1`**).

10 Haga clic en **Crear**.

Crear un puente de capa 2

Un puente de capa 2 permite que los nodos informáticos de una red de superposición se comuniquen con una VLAN física.

Crear un puente de capa 2 con NSX-T Data Center

Puede crear un puente de capa 2 en NSX-T Data Center a través de un clúster de puente.

Requisitos previos

En NSX-T Data Center, cree un clúster de puente que incluya dos hosts ESXi dedicados. Consulte "Crear un clúster de puente" en la *Guía de administración de NSX-T*.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Inicie sesión en el nodo del controlador como `viouser`.

3 Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su –
source ~/cloudadmin.rc
```

4 Cree una puerta de enlace de capa 2 lógica especificando el UUID del clúster de puente de NSX-T Data Center como el nombre del dispositivo.

```
neutron l2-gateway-create gateway-name --device name=bridge-cluster-uuid,interface_names="temp"
```

   Se omite el valor del nombre de la interfaz y el nombre se asigna automáticamente.

5 Cree la conexión de puerta de enlace de capa 2 lógica mediante la puerta de enlace que creó en el paso anterior.

```
neutron l2-gateway-connection-create gateway-name network-name --default-segmentation-id=vlan-id
```

Los nodos informáticos de la red de superposición ahora pueden acceder a la VLAN especificada.

Crear un puente de capa 2 con NSX Data Center for vSphere

Puede crear un puente de capa 2 en NSX-T Data Center a través de un grupo de puertos.

Requisitos previos

Cree un grupo de puertos y etiquételo con el identificador de la VLAN a la que desee conectar los nodos informáticos.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Inicie sesión en el nodo del controlador como `viouser`.

3 Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su -
source ~/cloudadmin.rc
```

4 Cree una puerta de enlace de capa 2 lógica especificando el identificador de objeto administrado (Managed Object Identifier, MOID) del grupo de puertos como el nombre de la interfaz.

```
neutron l2-gateway-create gateway-name --device name=temp,interface_names="portgroup-moid"
```

NSX Data Center for vSphere crea un enrutador lógico distribuido (Distributed Logical Router, DLR) dedicado a partir del grupo perimetral de copia de seguridad. Se omite el valor del nombre de dispositivo y se asigna automáticamente un nombre al objeto con el formato "L2 bridging-*gateway-id*".

5 Cree la conexión de puerta de enlace de capa 2 lógica mediante la puerta de enlace que creó en el paso anterior.

```
neutron l2-gateway-connection-create gateway-name network-name --default-segmentation-id=vlan-id
```

Los nodos informáticos de VXLAN ahora pueden acceder a la VLAN especificada.

Crear una zona de disponibilidad de Neutron

Las zonas de disponibilidad de Neutron permiten obtener una alta disponibilidad para recursos de red. Puede colocar nodos que ejecutan el mismo servicio en distintas zonas de disponibilidad para asegurarse de que el servicio no se interrumpa si se produce un error en una zona.

Crear una zona de disponibilidad de Neutron con NSX-T Data Center

Puede crear zonas de disponibilidad de Neutron adicionales con NSX-T Data Center actualizando la configuración de VMware Integrated OpenStack.

Requisitos previos

Cree un perfil de DHCP independiente y un servidor proxy de metadatos para cada zona de disponibilidad. Las zonas de disponibilidad pueden compartir un clúster perimetral o utilizar clústeres perimetrales independientes.

- Para obtener información sobre cómo crear un perfil de DHCP, consulte "Crear un perfil de servidor DHCP" en la *Guía de administración de NSX-T*.
- Para obtener información sobre la creación de un servidor proxy de metadatos, consulte "Agregar un servidor proxy de metadatos" en la *Guía de administración de NSX-T*.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

3. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
4. Quite la marca de comentario del parámetro `nsxv3_availability_zones` y establezca su valor como el nombre de la zona de disponibilidad que desea crear.

   El valor de este parámetro puede incluir varias zonas de disponibilidad. Separe varios nombres con comas (,).
5. Quite la marca de comentario del parámetro `nsxv3_availability_zones_detail` y configúrelo para la nueva zona de disponibilidad.

Opción	Descripción
zone_name	Introduzca el nombre de la zona de disponibilidad que desea configurar.
metadata_proxy	Introduzca el nombre o el UUID del servidor proxy de metadatos para la zona de disponibilidad.
dhcp_profile	Introduzca el nombre o el UUID del perfil de DHCP para la zona de disponibilidad.
native_metadata_route	(Opcional) Especifique la ruta que se utiliza para el servicio de proxy de metadatos. Introduzca una dirección IP con un prefijo en notación CIDR.
dns_domain	(Opcional) Introduzca el dominio DNS para nombres de host en la zona de disponibilidad.

Opción	Descripción
nameservers	(Opcional) Introduzca uno o varios servidores DNS con el fin de configurarlos para las entradas de enlace de DHCP.
default_overlay_tz	(Opcional) Introduzca el nombre o el UUID de la zona de transporte de superposición predeterminada.
default_vlan_tz	(Opcional) Introduzca el nombre o el UUID de la zona de transporte de VLAN predeterminada.
switching_profiles	(Opcional) Introduzca los UUID de los perfiles de conmutación para la zona de disponibilidad.
dhcp_relay_service	(Opcional) Introduzca el nombre o el UUID del servicio de retransmisión de DHCP para la zona de disponibilidad.
default_tier0_router	(Opcional) Introduzca el nombre o el UUID del enrutador de nivel 0 predeterminado para la zona de disponibilidad.

Asegúrese de que exista una copia de los parámetros anteriores para cada zona de disponibilidad configurada.

6 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

Se crea la nueva zona de disponibilidad. Con el fin de especificar una zona de disponibilidad para una red, incluya el parámetro `--availability-zone-hint` *az-name* al crear la red.

Ejemplo: Crear zonas de disponibilidad independientes para la ruta de acceso a datos estándar y mejorada de N-VDS

El siguiente procedimiento implementa las zonas de disponibilidad independiente para que pueda implementar cargas de trabajo de NFV en N-VDS en modo de ruta de acceso de datos mejorada y otras cargas de trabajo en el modo estándar. En este ejemplo, se ha implementado VMware Integrated OpenStack con NSX-T Data Center en el modo estándar. Las zonas de disponibilidad se configurarán en el mismo enrutador de nivel 0 y el clúster perimetral. La red de administración de VMware Integrated OpenStack utiliza el rango de direcciones IP de 192.0.2.10 a 192.0.2.50.

1 En NSX-T Data Center, configure una zona de transporte superpuesta y una zona de transporte de VLAN con N-VDS en el modo de ruta de acceso a datos mejorada. Consulte "Ruta de acceso a datos mejorada" en la *Guía de instalación de NSX-T Data Center*.

La zona de transporte superpuesta se denomina `nfv-overlay-tz` y la zona de transporte de VLAN se denomina `nfv-vlan-tz`.

2 Cree un perfil de DHCP para la nueva zona de disponibilidad.

a En NSX Manager, seleccione **Redes > DHCP**.

b En la pestaña **Perfiles de servidor**, haga clic en **Agregar**.

c Introduzca **`nfv dhcp`** para el nombre y seleccione el clúster perimetral existente.

d Haga clic en **Agregar**.

3 Cree un servidor proxy de metadatos para la nueva zona de disponibilidad.

a En NSX Manager, seleccione **Redes > DHCP**.

b En la pestaña **Proxies de metadatos**, haga clic en **Agregar**.

c Introduzca **`nfv mdp`** para el nombre.

d Introduzca **`http://192.0.2.10:8775`** para la dirección URL del servidor Nova.

e Introduzca **`mdpassword`** para el secreto.

f Seleccione el clúster perimetral existente.

g Haga clic en **Agregar**.

4 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

5 Abra el archivo `custom.yml` y agregue la siguiente información:

```
nsxv3_availability_zones: nfv-az
nsxv3_availability_zones_detail: [{'zone_name': 'nfv-az', 'metadata_proxy': 'nfv-mdp',
'dhcp_profile': 'nfv-dhcp', 'default_overlay_tz': 'nfv-overlay-tz', 'default_vlan_tz': 'nfv-vlan-
tz'},]
```

6 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

7 Crear una red en la nueva zona de disponibilidad.

a Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su -
source ~/cloudadmin.rc
```

b Cree la red.

```
neutron net-create nfv-network --tenant-id nfv-project --availability-zone-hint nfv-az
```

Crear una zona de disponibilidad de Neutron con NSX Data Center for vSphere

Puede crear zonas de disponibilidad de Neutron adicionales con NSX Data Center for vSphere actualizando la configuración de VMware Integrated OpenStack.

Requisitos previos

- Cree un clúster perimetral para la nueva zona de disponibilidad.
- Cree un grupo de recursos en el nuevo clúster perimetral.

- Configure el nuevo clúster perimetral para que utilice el conmutador distribuido adecuado. Si lo desea, puede crear un nuevo conmutador distribuido para la zona.
- En NSX Data Center for vSphere, cree una zona de transporte que incluya el nuevo clúster perimetral.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

3. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
4. Quite la marca de comentario del parámetro `nsxv_availability_zones` y establezca su valor como el nombre de la zona de disponibilidad que desea crear.

   El valor de este parámetro puede incluir varias zonas de disponibilidad. Separe varios nombres con comas (,).
5. Quite la marca de comentario del parámetro `nsxv_availability_zones_detail` y configúrelo para la nueva zona de disponibilidad.

Opción	Descripción
zone_name	Introduzca el nombre de la zona de disponibilidad que desea configurar.
resource_pool_id	Introduzca el identificador de objeto administrado (Managed Object Identifier, MOID) del grupo de recursos que creó para la nueva zona de disponibilidad.
datastore_id	Introduzca el MOID del almacén de datos que desea utilizar para la nueva zona de disponibilidad.
edge_ha	Introduzca **`True`** para habilitar la alta disponibilidad de los nodos perimetrales o **`False`** para deshabilitarla.
ha_datastore_id	Introduzca el MOID del almacén de datos que desea utilizar para la alta disponibilidad de los nodos perimetrales. Si establece `edge_ha` como `False`, no especifique ningún valor para el parámetro `ha_datastore_id`.
external_network	Introduzca el MOID del grupo de puertos de red externa en el conmutador distribuido para la nueva zona de disponibilidad.
vdn_scope_id	Introduzca el MOID de la zona de transporte que creó para la nueva zona de disponibilidad.
mgt_net_id	Introduzca el MOID de la red de administración para su implementación.

Opción	Descripción
mgt_net_proxy_ips	Introduzca las direcciones IP del servidor proxy de metadatos para su implementación.
dvs_id	Introduzca el MOID del conmutador distribuido para la nueva zona de disponibilidad.

Asegúrese de que exista una copia de los parámetros anteriores para cada zona de disponibilidad configurada.

6 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

Pasos siguientes

Con el fin de especificar una zona de disponibilidad para una red, incluya el parámetro `––availability–zone–hint` *az-name* al crear la red.

Configurar VMware Integrated OpenStack con un clúster de NSX Manager

NSX-T Data Center 2.4 y versiones posteriores admiten la implementación de varios nodos de NSX Manager para formar un clúster en una instancia única de NSX-T Data Center. Si desea utilizar un clúster de NSX Manager con VMware Integrated OpenStack, agregue las direcciones IP de todos los nodos del clúster a la configuración de implementación.

Nota Un clúster de NSX Manager proporciona alta disponibilidad para una instancia de NSX-T Data Center única. No se pueden utilizar varias instancias de NSX-T Data Center con la misma implementación de VMware Integrated OpenStack.

Requisitos previos

Cree el clúster de NSX Manager en NSX-T Data Center. Consulte "Implementar nodos de NSX Manager para formar un clúster desde la interfaz de usuario" en la *Guía de instalación de NSX-T Data Center*.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

3 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

4 Agregue el parámetro `nsxv3_api_managers` e incluya la dirección IP de cada nodo en el clúster NSX Manager.

```
nsxv3_api_managers: parent-manager-ip, manager-node2-ip,...
```

5 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

Pasos siguientes

Si cambia la dirección IP de cualquier nodo o si agrega o quita nodos del clúster de NSX Manager, debe modificar el archivo `custom.yml` para incluir la información de dirección IP que se actualizó.

Configurar la transparencia de VLAN

Las redes con transparencia de VLAN permiten que los paquetes etiquetados se transmitan sin quitar ni cambiar etiquetas.

Nota Para las implementaciones de VDS, solo las redes del proveedor pueden ser transparentes. Para las redes de NSX Data Center for vSphere y de NSX-T Data Center, solo las redes de tenant pueden ser transparentes.

Para habilitar la transparencia de VLAN en una red, incluya el parámetro `--transparent-vlan` y deshabilite la seguridad de puerto en la VLAN al crear la red. Por ejemplo:

```
openstack network create --project project-uuid --transparent-vlan --disable-port-security vlan-id
```

Configurar el aprendizaje de direcciones MAC

El aprendizaje de direcciones MAC habilita la conectividad de red para varias direcciones MAC detrás de una única vNIC. El aprendizaje de direcciones MAC resulta útil para distribuir cargas de trabajo en implementaciones de OpenStack de gran tamaño.

El aprendizaje de direcciones MAC en VMware Integrated OpenStack se implementa de manera diferente para las implementaciones de NSX-T Data Center y NSX Data Center for vSphere.

- Para las implementaciones de NSX-T Data Center, NSX-T Data Center proporciona el aprendizaje de direcciones MAC en VMware Integrated OpenStack. Para obtener más información, consulte "Descripción del perfil de conmutación de administración de MAC" en la *Guía de administración de NSX-T*.
- Para las implementaciones de NSX Data Center for vSphere, el aprendizaje de direcciones MAC en VMware Integrated OpenStack se implementa mediante la habilitación de la transmisión manipulada y el modo promiscuo. El invitado debe solicitar el modo promiscuo.

Se aplican las siguientes condiciones al aprendizaje de direcciones MAC:

- El aprendizaje de direcciones MAC no es compatible con la seguridad del puerto o los grupos de seguridad.
- Para las implementaciones de NSX Data Center for vSphere, el rendimiento se verá afectado debido a que las vNIC que solicitan el modo promiscuo reciben una copia de cada paquete.
- Para las implementaciones de NSX Data Center for vSphere, no se generan solicitudes RARP para varias direcciones MAC detrás de una sola vNIC cuando se migra una máquina virtual con vMotion. Esto puede provocar una pérdida de conectividad.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su -
source ~/cloudadmin.rc
```

3. Deshabilite la seguridad del puerto y los grupos de seguridad en el puerto en el que desea configurar el aprendizaje de direcciones MAC.

```
neutron port-update port-uuid --port-security-enabled false --no-security-groups
```

4. Habilite el aprendizaje de direcciones MAC en el puerto.

```
neutron port-update port-uuid --mac-learning-enabled true
```

Administrar HA perimetral con NSX Data Center for vSphere

Para las implementaciones de NSX Data Center for vSphere, puede habilitar HA en los nodos de NSX Edge y especificar los grupos de hosts en los que se colocarán los nodos.

Requisitos previos

- Compruebe que el clúster perimetral tenga al menos dos hosts. De lo contrario, podría recibir un error de antiafinidad.
- Si desea especificar grupos de host perimetrales, cree y configure los grupos de hosts en vSphere.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

3 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

4 Quite la marca de comentario del parámetro `nsxv_edge_ha` y establezca su valor como **`True`**.

5 Si desea utilizar grupos de hosts perimetrales, quite la marca de comentario del parámetro `nsxv_edge_host_groups` y establezca su valor como los dos grupos de hosts perimetrales que creó separados una coma (,).

6 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

7 Inicie sesión en el nodo del controlador como `viouser`.

8 Si especifica grupos de host, actualice el entorno para incluirlos.

```
sudo –u neutron nsxadmin –o nsx–update –r edges ––property hostgroup=all
```

9 Si el entorno ya incluye nodos de NSX Edge, habilite HA en esos nodos y mígrelos a los grupos de hosts especificados.

a Habilite la alta disponibilidad en cada nodo de NSX Edge existente.

```
sudo –u neutron nsxadmin –r edges –o nsx–update ––property highAvailability=True ––property
edge–id=edge–node–id
```

Para buscar el identificador de un nodo de NSX Edge, puede ejecutar el comando `sudo –u neutron nsxadmin –r edges –o nsx–list`.

b Migre todos los nodos perimetrales existentes a los grupos de hosts especificados.

```
sudo –u neutron nsxadmin –r edges –o nsx–update ––property hostgroup=all
```

Si solo desea migrar nodos perimetrales concretos, puede utilizar el siguiente comando:

```
sudo –u neutron nsxadmin –o nsx–update –r edges –p edge–id=edge–node–id –p hostgroup=True
```

HA de Edge se habilita para los nodos que desee. Si especificó grupos de hosts perimetrales, se crean nodos perimetrales actuales y futuros de esos grupos.

Pasos siguientes

Puede actualizar los grupos de hosts perimetrales en `custom.yml` después de la configuración original. Después de implementar `custom.yml`, ejecute los siguientes comandos para actualizar el entorno:

```
sudo –u neutron nsxadmin –o nsx–update –r edges ––property hostgroup=clean
sudo –u neutron nsxadmin –o nsx–update –r edges ––property hostgroup=all
```

A continuación, vuelva a realizar el paso 9 para migrar los nodos perimetrales a los nuevos grupos de hosts.

Especificar los tipos de enrutador de tenant para NSX Data Center for vSphere

Para las implementaciones de NSX Data Center for vSphere, puede restringir los tipos de enrutador disponibles para los tenants y especificar un tipo de enrutador predeterminado.

Nota Los administradores pueden crear enrutadores de cualquier tipo.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

3. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
4. Quite la marca de comentario del parámetro `nsxv_tenant_router_types` y especifique los tipos de enrutador que desea poner a disposición de los tenants.

   Puede introducir **`exclusive`**, **`shared`**, **`distributed`** o cualquier combinación de estos separada por comas (,).

   Los valores del parámetro `nsxv_tenant_router_types` se utilizan en orden como los tipos de enrutador predeterminados.
5. Implemente la configuración actualizada.

   ```
   sudo viocli deployment configure
   ```

   Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

Los tenants solo pueden crear enrutadores de los tipos enumerados. Si un tenant crea un enrutador sin especificar un tipo, se utilizará el primer tipo disponible de forma predeterminada.

Configurar el enrutamiento dinámico para redes de Neutron con NSX Data Center for vSphere

Puede configurar el enrutamiento dinámico de BGP para las redes de proveedor y de tenant en el entorno.

Después de habilitar BGP, las subredes lógicas creadas por los tenants se anuncian fuera del entorno sin que sea necesario indicar el NAT de origen o las direcciones IP flotantes. Primero debe crear una red externa de VXLAN que más adelante utilizará como interfaz interna para las instancias de Edge de puerta de enlace.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Inicie sesión en el nodo del controlador como `viouser`.

3 Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su –
source ~/cloudadmin.rc
```

4 Cree un ámbito de dirección IPv4 para futuras subredes de tenants y la subred de la red VXLAN externa.

```
neutron address-scope-create name 4
```

5 Cree un grupo de subredes para la red externa.

```
neutron subnetpool-create external-pool --pool-prefix network-address --default-prefixlen prefix-bits --address-scope scope-name --shared
```

Opción	Descripción
external-pool	Introduzca un nombre para el grupo de subredes.
--pool-prefix	Introduzca la dirección de red del grupo de subredes en formato CIDR (por ejemplo, 192.0.2.0/24). Las subredes se asignarán desde esta red.
--default-prefixlen	Introduzca la longitud del prefijo de red (en bits) para utilizarlo con nuevas subredes que se crean sin especificar una longitud de prefijo.
--address-scope	Introduzca el nombre del ámbito de dirección IPv4 que creó en el paso 4.

6 Cree un grupo de subredes para redes de tenants.

```
neutron subnetpool-create tenant-pool --pool-prefix network-address --default-prefixlen prefix-bits --address-scope scope-name --shared
```

Nota OpenStack anunciará este grupo de subredes al tejido físico. Especifique un prefijo que no se esté utilizando actualmente.

Opción	Descripción
tenant-pool	Introduzca un nombre para el grupo de subredes.
--pool-prefix	Introduzca la dirección de red del grupo de subredes en formato CIDR (por ejemplo, 192.51.100.0/24). Las subredes se asignarán desde esta red.
--default-prefixlen	Introduzca la longitud del prefijo de red (en bits) para utilizarlo con nuevas subredes que se crean sin especificar una longitud de prefijo.
--address-scope	Introduzca el nombre del ámbito de dirección IPv4 que creó en el paso 4.

7 Cree una red externa basada en VXLAN.

```
neutron net-create network-name --provider:network_type vxlan --router:external
```

Este comando crea un nuevo conmutador lógico en NSX Data Center for vSphere.

8 Crear una subred en la red externa.

La subred debe tener deshabilitado DHCP y ninguna puerta de enlace.

```
neutron subnet-create external-network external-subnet-address --name external-subnet --allocation-pool start=subnet-ip1,end=subnet-ip2 --subnetpool provider-subnet-pool --no-gateway --disable-dhcp
```

Opción	Descripción
external-network	Introduzca el nombre de la red externa basada en VXLAN que creó en el paso 7.
external-subnet-address	Introduzca la dirección de red de la subred en formato CIDR (por ejemplo, 192.51.100.0/28).
--name	Introduzca un nombre para la subred.
--allocation-pool	Introduzca la primera y la última dirección IP del rango que desea asignar de esta subred.
--subnetpool	Introduzca el grupo de subredes que creó en el paso 5 para la red externa.

9 Cree nodos perimetrales de BGP.

```
sudo -u neutron nsxadmin -r bgp-gw-edge -o create --property name=edge-name --property local-as=local-as-number --property external-iface=portgroup-moid:mgmt-network-ip --property internal-iface=physical-net-id:external-network-ip
```

Opción	Descripción
name	Introduzca un nombre para el nodo perimetral de BGP.
local-as	Introduzca el número de AS local para el nodo perimetral. Los enrutadores físicos y perimetrales no pueden estar en el mismo AS.
external-iface	Introduzca el identificador de objeto administrado (Managed Object Identifier, MOID) del grupo de puertos asociado con la VLAN que conecta los nodos perimetrales con los enrutadores físicos. Después de los dos puntos, introduzca la dirección IP del nodo perimetral en la red de administración.
internal-iface	Introduzca el identificador de cableado virtual de la red externa basada en VXLAN. Después de los dos puntos, introduzca la dirección IP del nodo perimetral en la red física. Para buscar el identificador de cableado virtual, ejecute el comando `openstack network show external-network-name` y busque el valor del parámetro `provider:physical_network`.

10 Habilite el anuncio de BGP en los nodos perimetrales.

```
sudo -u neutron nsxadmin -r routing-redistribution-rule -o create --property gw-edge-ids=edge1-id,edge2-id --property learner-protocol=bgp --property learn-from=connected,bgp --property action=permit
```

Para el parámetro `gw-edge-ids`, utilice el identificador perimetral (por ejemplo, `edge-4`) en lugar del nombre. Puede ejecutar el comando `sudo -u neutron nsxadmin -r bgp-gw-edge -o view` para mostrar el identificador de cada nodo perimetral de BGP.

11 Establezca una relación de vecino de BGP entre los nodos perimetrales.

```
sudo -u neutron nsxadmin -r bgp-neighbour -o create --property gw-edge-ids=edge1-id,edge2-id --property ip-address=physical-router1-ip --property remote-as=remote-as-number --property password=bgp-password
```

Opción	Descripción
gw-edge-ids	Introduzca el identificador perimetral de cada nodo, separado por comas.
ip-address	Introduzca la dirección IP en el enrutador físico.
remote-as	Introduzca el número de AS de los enrutadores físicos conectados a los nodos perimetrales.
password	Introduzca la contraseña de BGP.

12 Configure los enrutadores físicos.

a Asegúrese de que el AS de los enrutadores físicos es el AS remoto de los nodos perimetrales.

b Configure los nodos perimetrales como vecinos de BGP.

c Configure cada enrutador de modo que se anuncie como una puerta de enlace dinámica.

13 Cree y configure el orador de BGP.

a Cree BGP Speaker.

```
neutron bgp-speaker-create --local-as local_as_value name_bgp_speaker
```

b Cree los emparejamientos de BGP.

```
neutron bgp-peer-create --peer-ip internal_interface_network_GW-EDGE1 --remote-as 65001 --
password BGP_password --auth-type md5 name_GW-EDGE1 --esg-id edge-ID_GW-EDGE1

neutron bgp-peer-create --peer-ip internal_interface_network_GW-EDGE2 --remote-as 65001 --
password BGP_password --auth-type md5 name_GW-EDGE2 --esg-id edge-ID_GW-EDGE2
```

c Agregue el emparejamiento de BGP a BGP Speaker.

```
neutron bgp-speaker-peer-add name_bgp_speaker name_GW-EDGE1

neutron bgp-speaker-peer-add name_bgp_speaker name_GW-EDGE2
```

d Asocie Speaker con la red VXLAN.

```
neutron bgp-speaker-network-add name_bgp_speaker external_VXLAN_network_name
```

14 (opcional) Cree enrutadores de BGP para los arrendatarios.

Los usuarios de arrendatario pueden crear sus propios enrutadores de BGP. El usuario de arrendatario debe ser `admin` para configurar un enrutador sin SNAT.

a Cree dos conmutadores lógicos para un arrendatario y grupos de subredes para ellos.

```
neutron net-create name_Tenant1_LS1

neutron subnet-create --name name_network_Tenant1-LS1 name_Tenant1_LS1 --subnetpool selfservice

neutron net-create name_Tenant1_LS2

neutron subnet-create --name name_network_Tenant1-LS2 name_Tenant1_LS2 --subnetpool selfservice
```

b Cree un enrutador con la configuración de BGP.

BGP funciona con todos los formatos de enrutadores lógicos de OpenStack: `shared`, `distributed` y `exclusive`.

```
neutron router-create name_Tenant1-LR --router_type=exclusive

neutron router-interface-add name_Tenant1-LR name_network_Tenant1-LS1

neutron router-interface-add name_Tenant1-LR name_network_Tenant1-LS2

neutron router-gateway-set name_Tenant1-LR --disable-snat external_VXLAN_network_name
```

El enrutamiento dinámico de BGP ahora está configurado en el lado del proveedor y los arrendatarios también pueden utilizarlo.

Agregar un back-end de NSX-T Data Center a una implementación de NSX Data Center for vSphere

Si se implementó VMware Integrated OpenStack con NSX Data Center for vSphere, puede especificar un back-end de NSX-T Data Center para determinados proyectos en la implementación.

Importante Este proceso actualizará el archivo `custom.yml` o generará automáticamente un archivo `custom.yml` si el archivo no existe en el entorno. Después de ejecutar el comando `viocli enable-tvd`, no elimine `custom.yml` o se descartará la configuración. Para obtener más información, consulte Comando viocli enable-tvd.

Requisitos previos

- Implemente VMware Integrated OpenStack con redes de NSX Data Center for vSphere.
- Implemente NSX-T Data Center y obtenga los siguientes parámetros:
  - Dirección IP de NSX Manager
  - Nombre de usuario y contraseña para acceder a NSX Manager

- Zona de transporte de superposición
- Zona de transporte de VLAN
- Enrutador de nivel 0
- Perfil de DHCP
- Servidor proxy de metadatos

Procedimiento

1 Cree clústeres de proceso para todos los proyectos para los que desea usar NSX-T Data Center y configure esos clústeres como nodos de transporte en el entorno de NSX-T Data Center.

   Un clúster de proceso no puede formar parte de una implementación de NSX Data Center for vSphere y NSX-T Data Center al mismo tiempo.

2 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

3 Habilite el complemento de TVD.

```
sudo viocli enable-tvd --nsx-mgr manager-ip --nsx-user username --nsx-passwd password [--nsx-insecure {true | false}] [--nsx-ca-file ca-file] [--nsx-overlay-tz overlay-zone] [--nsx-vlan-tz vlan-zone] [--nsx-tier0-rt t0-router] [--nsx-dhcp-profile profile] [--nsx-md-proxy mdp-server]
```

Opción	Descripción
--nsx-mgr	Introduzca la dirección IP de la instancia de NSX Manager de la implementación de NSX-T Data Center.
--nsx-user	Introduzca el nombre de usuario del administrador de NSX Manager.
--nsx-passwd	Introduzca la contraseña del administrador de NSX Manager.
--nsx-insecure {true | false}	Especifique si se debe comprobar el certificado del servidor de NSX Manager. El valor predeterminado es `true`.
--nsx-ca-file	Especifique el archivo de paquete de CA que se utilizará para comprobar el certificado del servidor de NSX Manager. Este parámetro se ignora si establece `--nsx-insecure` en `true`.
--nsx-overlay-tz	Introduzca el nombre o el UUID de la zona de transporte de superposición de NSX-T Data Center predeterminada que se emplea para crear redes de Neutron aisladas de túnel.
--nsx-vlan-tz	Introduzca el nombre o el UUID de la zona de transporte de VLAN de NSX-T Data Center predeterminada que se emplea para establecer puentes entre las redes de Neutron si no se especificó ninguna red física.
--nsx-tier0-rt	Introduzca el nombre o el UUID del enrutador de nivel 0 predeterminado que se emplea para conectarse a enrutadores lógicos de nivel 1 y configurar redes externas.
--nsx-dhcp-profile	Introduzca el nombre o el UUID del perfil de DHCP de NSX-T Data Center empleado para habilitar el servicio DHCP nativo.
--nsx-md-proxy	Introduzca el nombre o el UUID del servidor proxy de metadatos de NSX-T Data Center usado para habilitar el servicio de metadatos nativo.

4 Asigne proyectos existentes al back-end de NSX-T Data Center o NSX Data Center for vSphere.

- Para crear asignaciones de proyecto desde la CLI de Servidor de administración de OpenStack, ejecute el siguiente comando:

```
openstack project plugin create project-uuid --plugin {nsx-v | nsx-t}
```

- Para crear asignaciones de proyecto desde el panel de control de VMware Integrated OpenStack, realice los siguientes pasos:
  a Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube y seleccione el proyecto admin del menú desplegable en la barra de título.
  b Seleccione **Administrador > Proyecto > Asignación de complemento de proyecto**.
  c Haga clic en **Crear asignación de proyecto**.
  d Especifique el proyecto y el back-end que desee, y haga clic en **Enviar**.

Los proyectos sin una asignación utilizan el back-end de NSX Data Center for vSphere de forma predeterminada.

Autenticación e identidad

4

En VMware Integrated OpenStack, el componente de Keystone proporciona autenticación y administración de identidades. Además de los usuarios de OpenStack compatible con SQL, también puede configurar la autenticación a través de LDAP o a través de la federación de identidades.

VMware Integrated OpenStack admite la federación de identidades con VMware Identity Manager como proveedor de identidad. También puede implementar la federación con un proveedor de identidad de terceros a través del protocolo SAML 2.0, pero esto no es compatible con VMware.

Este capítulo incluye los siguientes temas:

Administración de dominios

Puede crear dominios para administrar usuarios y tenants.

Todas las implementaciones de VMware Integrated OpenStack contienen los dominios `local` y `Default`.

- El dominio `local` incluye usuarios de servicio y está respaldado por una base de datos de SQL local.
- El dominio `Default` contiene usuarios estándar de OpenStack. Si configura LDAP durante la instalación de VMware Integrated OpenStack (un solo dominio), el dominio `Default` está respaldado por LDAP y también contiene los usuarios de LDAP. De lo contrario, `Default` está respaldado por la base de datos local de SQL.
- El usuario de `admin` es miembro de los dominios `local` y `Default`.

Importante No deshabilite ni elimine los dominios `local` o `Default`.

Puede crear y administrar dominios adicionales según sea necesario. Por ejemplo, puede crear un dominio independiente para usuarios federados. Para administrar los dominios, seleccione **Identidad > Dominios** en el panel de control de VMware Integrated OpenStack.

Configurar autenticación LDAP

Puede configurar la autenticación LDAP o modificar la configuración de LDAP existente.

VMware Integrated OpenStack admite SQL y uno o varios dominios como origen de identidad (hasta un máximo de 10 dominios).

Importante Todos los atributos de LDAP deben usar caracteres ASCII únicamente.

Requisitos previos

Póngase en contacto con el administrador de LDAP o utilice herramientas como ldapsearch o Apache Directory Studio para obtener los valores correctos para la configuración de LDAP.

Procedimiento

1. En vSphere Client, seleccione **Menú > VMware Integrated OpenStack**.
2. Haga clic en **Implementaciones de OpenStack** y abra la pestaña **Administración**.
3. En la pestaña **Configuración**, haga clic en **Configurar el origen de identidad**.
4. Haga clic en el icono **Agregar** (signo más) para configurar un nuevo origen de LDAP o en el icono **Editar** (lápiz) para modificar una configuración existente.
5. Introduzca la configuración de LDAP.

Opción	Descripción
Nombre de dominio de Active Directory	Especifique el nombre de dominio completo de Active Directory.
Nombre de dominio de Keystone	Introduzca el nombre de dominio de Keystone. No utilice `default` ni `local` como un dominio de Keystone.
Usuario de enlace	Introduzca el nombre de usuario para el enlace con Active Directory para las solicitudes de LDAP.
Contraseña de enlace	Introduzca la contraseña con la cual el cliente LDAP pueda acceder al servidor LDAP.
Controladores de dominio	(Opcional) Introduzca las direcciones IP de uno o varios controladores de dominio separadas por comas (,). Si no especifica los controladores de dominio, VMware Integrated OpenStack elegirá automáticamente un controlador de dominio de Active Directory existente.
Sitio	(Opcional) Introduzca un sitio de implementación específico dentro de la organización para limitar la búsqueda de LDAP a ese sitio.
DN de árbol de usuario	(Opcional) Introduzca la base de búsqueda para los usuarios (por ejemplo, **`DC=vmware, DC=com`**). En la mayoría de las implementaciones de Active Directory, se utiliza la parte superior del árbol de usuario de forma predeterminada.

Opción	Descripción
Filtro de usuario	(Opcional) Introduzca un filtro de búsqueda de LDAP para los usuarios. Establezca la configuración del dominio de AD para filtrar los usuarios con el mismo nombre que los usuarios de servicio de OpenStack como nova o cinder. **Importante** Si el directorio contiene más de 1.000 objetos (usuarios y grupos), debe aplicar un filtro para garantizar que se devuelvan menos de 1.000 objetos. Para obtener más información sobre los filtros, consulte https://docs.microsoft.com/en-us/windows/desktop/ADSI/search-filter-syntax.
DN de árbol de grupo	(Opcional) Introduzca la base de búsqueda para los grupos. El sufijo LDAP se utiliza de forma predeterminada.
Filtro de grupo	(Opcional) Introduzca un filtro de búsqueda de LDAP para los grupos.
Usuario administrador de LDAP	Si el proveedor de identidad de Keystone está configurado para funcionar con OpenLDAP, introduzca el usuario administrador de LDAP.

Puede activar la casilla **Configuración avanzada** para mostrar los campos adicionales de configuración de LDAP.

Opción	Descripción
Cifrado	Seleccione **Ninguno**, **SSL**o **StartTLS**.
Nombre del host	Introduzca el nombre del host del servidor LDAP.
Puerto	Introduzca el número de puerto para usarlo en el servidor LDAP.
Atributo objectclass para usuario	(Opcional) Introduzca una clase de objeto LDAP para los usuarios.
Atributo de ID de usuario	(Opcional) Introduzca el atributo de LDAP asignado al identificador de usuario. Este valor no puede ser un atributo con varios valores.
Atributo de nombre de usuario	(Opcional) Introduzca el atributo de LDAP asignado al nombre de usuario.
Atributo de correo de usuario	(Opcional) Introduzca el atributo de LDAP asignado al correo electrónico de usuario.
Atributo de contraseña de usuario	(Opcional) Introduzca el atributo de LDAP asignado a la contraseña.
Atributo objectclass para grupo	(Opcional) Introduzca la clase de objeto de LDAP para grupos.
Atributo de ID de grupo	(Opcional) Introduzca el atributo de LDAP asignado al identificador de grupo.
Atributo de nombre de grupo	(Opcional) Introduzca el atributo de LDAP asignado al nombre de grupo.
Atributo de miembro de grupo	(Opcional) Introduzca el atributo de LDAP asignado al nombre de miembro de grupo.
Atributo de descripción de grupo	(Opcional) Introduzca el atributo de LDAP asignado a la descripción de grupo.

6 Haga clic en el botón **Validar** para confirmar la configuración.

La validación comprueba que existe el usuario administrador y que los usuarios están disponibles en el DN de árbol de usuario y la búsqueda con filtro.

7 Haga clic en **Aceptar**.

Configurar la federación de VMware Identity Manager

Puede configurar VMware Integrated OpenStack para utilizar VMware Identity Manager como una solución de proveedor de identidad.

Los usuarios pueden autenticarse con VMware Identity Manager a través del protocolo de lenguaje de marcado de asociación de seguridad (Security Association Markup Language, SAML) 2.0 o el protocolo OpenID Connect (OIDC).

- Los usuarios de SAML 2.0 deben autenticarse mediante el panel de control de VMware Integrated OpenStack. La interfaz de línea de comandos de OpenStack no es compatible con SAML 2.0.
- Los usuarios de OpenID Connect pueden autenticarse en el panel de control de VMware Integrated OpenStack o en la interfaz de línea de comandos de OpenStack.

Requisitos previos

- Implemente y configure VMware Identity Manager 3.3 o posterior.
- Asegúrese de que su instancia de VMware Identity Manager puede comunicarse con la red de administración de VMware Integrated OpenStack.

Nota Una implementación de VMware Integrated OpenStack puede incluir solo un proveedor de identidad federada. Puede ejecutar `viocli federation identity-provider list` para mostrar todos los proveedores de identidad configurados y `viocli federation identity-provider remove` para quitarlos por identificador.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Agregue VMware Identity Manager como proveedor de identidad.

```
sudo viocli federation identity-provider add --type vidm
```

3. Introduzca la siguiente información cuando se le solicite.

Opción	Descripción
Nombre del proveedor de identidad	Escriba un nombre para el proveedor de identidad. Este nombre se utiliza en las operaciones de la línea de comandos de Servidor de administración de OpenStack y no puede incluir caracteres especiales ni espacios.
Nombre para mostrar del proveedor de identidad (para Horizon)	Introduzca un nombre para mostrar para el proveedor de identidad. Este nombre se muestra a los usuarios en **Autenticar usando** cuando inician sesión en el panel de control de VMware Integrated OpenStack.
Descripción	(Opcional) Introduzca una descripción del proveedor de identidad.
Dirección del endpoint de vIDM	Escriba el FQDN de la instancia de VMware Identity Manager (por ejemplo, `https://vxlan-vm-2-10.network.example.com`).
Usuario administrador de vIDM	Introduzca el nombre de usuario de un administrador de VMware Identity Manager.
Contraseña de administrador de vIDM	Introduzca la contraseña del administrador de VMware Identity Manager.
No comprobar certificados al establecer conexiones TLS/SSL	Introduzca **`false`** para comprobar los certificados de TLS o **`true`** para deshabilitar la comprobación de certificados.

Opción	Descripción
Nombre de tenant de vIDM	Si utiliza VMware Identity Manager dentro de una implementación de vRealize Automation, introduzca **`vsphere.local`**. De lo contrario, deje el valor en blanco y presione Entrar.
Introducir el nombre del dominio con el que se asocian los usuarios federados	Escriba el dominio de Keystone al que pertenecerán todos los usuarios federados. Si no existe, se creará el dominio.
Introducir el nombre de los grupos con los que se asocian los usuarios federados (separados por coma ",")	Escriba uno o más grupos que contengan usuarios federados. Si desea utilizar asignaciones personalizadas, introduzca todos los grupos que se incluyen en el archivo de asignación. Si no existen, se crearán los grupos que especifique.
¿Desea habilitar la compatibilidad con OpenID Connect?	Introduzca **`false`** para utilizar SAML o **`true`** para utilizar OpenID Connect.
¿Desea habilitar el flujo de trabajo de la API de OAuth?	Introduzca **`false`** para utilizar SAML o **`true`** para utilizar OpenID Connect.
¿Desea cambiar la configuración avanzada?	Introduzca **`n`**.

4 Implemente la configuración de identidad actualizada.

```
sudo viocli identity configure
```

Al implementar la configuración de identidad, se interrumpen brevemente los servicios de OpenStack.

VMware Integrated OpenStack está integrado con VMware Identity Manager, y los grupos y usuarios federados se importan en OpenStack. Cuando acceda al panel de control de VMware Integrated OpenStack, podrá elegir el proveedor de identidad VMware Identity Manager para iniciar sesión como un usuario federado.

Configurar la federación de SAML 2.0 genérica

Es posible integrar VMware Integrated OpenStack con cualquier solución de proveedor de identidad de terceros que use el protocolo de lenguaje de marcado de asociación de seguridad (Security Association Markup Language, SAML) 2.0.

Importante Los proveedores de identidad de terceros no son compatibles con VMware. Póngase en contacto con el administrador del proveedor de identidad para obtener la información necesaria para este procedimiento.

Si desea integrar VMware Integrated OpenStack con VMware Identity Manager mediante SAML 2.0, consulte Configurar la federación de VMware Identity Manager.

Requisitos previos

- Implemente la solución de proveedor de identidad y determine la ubicación de su archivo de metadatos.
- Asegúrese de que el nodo del controlador de VMware Integrated OpenStack puede acceder al FQDN de la solución de proveedor de identidad.

- Cree un archivo de asignación en formato JSON y guárdelo en el Servidor de administración de OpenStack. Para obtener más información, consulte "Asignación de combinaciones" en la documentación de OpenStack en https://docs.openstack.org/keystone/queens/advanced-topics/federation/mapping_combinations.html.
- Cree un archivo de asignación de atributos SAML en formato JSON y guárdelo en el Servidor de administración de OpenStack. Utilice la estructura siguiente:

```
[
    {
        "name": "attribute-1",
        "id": "id-1"
    },
    {
        "name": "attribute-2",
        "id": "id-2"
    },
    ...
]
```

Nota Una implementación de VMware Integrated OpenStack puede incluir solo un proveedor de identidad federada. Puede ejecutar `viocli federation identity-provider list` para mostrar todos los proveedores de identidad configurados y `viocli federation identity-provider remove` para quitarlos por identificador.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Agregue su solución de proveedor de identidad a VMware Integrated OpenStack.

```
sudo viocli federation identity-provider add --type saml2
```

3. Introduzca la siguiente información cuando se le solicite.

Opción	Descripción
Nombre del proveedor de identidad	Escriba un nombre para el proveedor de identidad. Este nombre se utiliza en las operaciones de la línea de comandos de Servidor de administración de OpenStack y no puede incluir caracteres especiales ni espacios.
Nombre para mostrar del proveedor de identidad (para Horizon)	Introduzca un nombre para mostrar para el proveedor de identidad. Este nombre se muestra a los usuarios en **Autenticar usando** cuando inician sesión en el panel de control de VMware Integrated OpenStack.
Descripción	(Opcional) Introduzca una descripción del proveedor de identidad.
¿Desea utilizar la dirección URL o el archivo local para los metadatos de IdP?	Introduzca **`url`**. No se admite la obtención de metadatos del proveedor de identidad desde un archivo local.
URL de metadatos de IdP	Introduzca la dirección URL en el archivo de metadatos del proveedor de identidad (por ejemplo, `https://idp-fqdn/metadata.xml`). Debe especificar el proveedor de identidad por FQDN.

Opción	Descripción
No comprobar certificados al establecer conexiones TLS/SSL	Introduzca **`false`** para comprobar los certificados de TLS o **`true`** para deshabilitar la comprobación de certificados.
¿Desea utilizar un archivo de plantilla o un archivo estático para reglas de asignación?	Introduzca **`static`** para utilizar un archivo de asignación estático o **`template`** para utilizar una plantilla de asignación.
Introducir la ruta local del archivo de reglas de asignación	Introduzca la ruta de acceso al archivo de reglas de asignación en el sistema local.
Introducir el nombre del dominio con el que se asocian los usuarios federados	Escriba el dominio de Keystone al que pertenecerán los usuarios federados. Si no existe, se creará el dominio.
Introducir el nombre de los grupos con los que se asocian los usuarios federados (separados por coma ",")	Escriba uno o más grupos para crearlos para los usuarios federados. Debe introducir todos los grupos que están incluidos en el archivo de asignación. Si no existen, se crearán los grupos que especifique.
¿Desea utilizar un archivo de plantilla o un archivo estático para la asignación de atributo?	Introduzca **`static`** para utilizar un archivo de asignación estático o **`template`** para utilizar una plantilla de asignación.
Introducir la ruta local del archivo de asignación de atributo	Introduzca la ruta del archivo de asignación de atributo en el sistema local.

4 Implemente la configuración de identidad actualizada.

```
sudo viocli identity configure
```

Al implementar la configuración de identidad, se interrumpen brevemente los servicios de OpenStack.

VMware Integrated OpenStack se integra con la solución de proveedor de identidad, y los grupos y los usuarios federados se importan en OpenStack. Cuando acceda al panel de control de VMware Integrated OpenStack, podrá elegir el proveedor de identidad especificado para iniciar sesión como un usuario federado.

Ejemplo: Ejemplo: Integrar VMware Integrated OpenStack con los servicios de federación de Active Directory

En el siguiente procedimiento se implementa la federación de identidades entre VMware Integrated OpenStack y los servicios de federación de Active Directory (Active Directory Federation Services, AD FS). En este ejemplo, la dirección IP virtual pública de la implementación de VMware Integrated OpenStack es `192.0.2.160` y la función de AD FS se agregó a una máquina virtual de Windows Server ubicada en `adfs.example.com`.

1 En AD FS, agregue una relación de confianza para usuario autenticado para VMware Integrated OpenStack.

a En **Administración de AD FS**, seleccione **Acción > Agregar veracidad del usuario de confianza...**.

b Haga clic en **Iniciar**.

c Seleccione **Escribir manualmente los datos sobre el usuario de confianza** y haga clic en **Siguiente**.

d Introduzca **`OpenStack`** para el nombre para mostrar y haga clic en **Siguiente**.

e Seleccione **Perfil de AD FS** y haga clic en **Siguiente**.

f Haga clic en **Siguiente**.

g Seleccione **Habilitar compatibilidad con el protocolo SAML 2.0 WebSSO**.

h Introduzca **`https://192.0.2.160:5000/saml`** para la dirección URL del usuario de confianza y haga clic en **Siguiente**.

i Introduzca **`https://192.0.2.160:5000/saml`** para el identificador de la relación de confianza para usuario autenticado, haga clic en **Agregar** y luego en **Siguiente**.

j Seleccione **No deseo establecer la configuración de autenticación multifactor** y haga clic en **Siguiente**.

k Seleccione **Permitir que todos los usuarios tengan acceso a este usuario de confianza** y haga clic en **Siguiente**.

l Haga clic en **Siguiente**, seleccione **Editar reglas de notificación** y haga clic en **Cerrar**.

m Haga clic en **Agregar regla...**.

n Seleccione **Establecer acceso directo de una notificación entrante o filtrarla** y haga clic en **Siguiente**.

o Introduzca un **Acceso directo de UPN** para el nombre de regla y seleccione **UPN** para el tipo de notificación entrante.

p Seleccione **Establecer acceso directo de todos los valores de notificaciones** y haga clic en **Finalizar**.

2 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

3 Escriba la siguiente información en un archivo denominado `mapping.json`.

```
[
    {
        "local": [
            {
                "user": {
                    "name": "{0}",
                },
                "group": {
                    "domain": {
                        "name": "adfs-users"
                    },
                    "name": "Federated Users"
                }
            }
        ],
        "remote": [
```

```
            {
                "type": "upn"
            }
        ]
    }
]
```

4 Escriba la siguiente información en un archivo denominado `attribute.json`.

```
[
    {
        "name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn",
        "id": "upn"
    }
]
```

5 Agregue AD FS como proveedor de identidad.

```
sudo viocli federation identity-provider add --type saml2
```

6 Introduzca la información que se le solicite.

```
Identity provider name []: adfs
Identity provider display name (for Horizon) []: Active Directory Federation Services
Description []: ADFS deployment
Do you wish to use URL or local file for IdP metadata? (url, file) [url]: url
IdP metadata URL []: https://adfs.example.com/federationmetadata/2007-06/federationmetadata.xml
Do not verify certificates when establishing TLS/SSL connections [False]: false
Do you wish to use a static file or template file for mapping rules? (static, template) [static]:
static
Enter the local path of mapping rules file: mapping.json
Enter the name of the domain that federated users associate with [Default]: adfs-users
Enter the name to the groups that federated users associate with (separated by commas ",") []:
Federated Users
Do you wish to use a static file or template file for attribute mapping? (static, template)
[static]: static
Enter the local path of attribute mapping file: attribute.json
```

7 Implemente la configuración de identidad actualizada.

```
sudo viocli identity configure
```

Después de implementar la configuración, abra el panel de control de VMware Integrated OpenStack. Ya puede seleccionar el proveedor de identidad de AD FS e iniciar sesión como un usuario federado.

Proyectos y usuarios de OpenStack 5

En VMware Integrated OpenStack, los administradores de nube gestionan los permisos a través de definiciones de usuario, grupo y proyecto. Los proyectos de OpenStack equivalen a los arrendatarios de vCloud Suite. Puede controlar la seguridad de red en el nivel de proyecto mediante las directivas de seguridad de NSX Data Center for vSphere o los grupos de seguridad del proveedor.

Este capítulo incluye los siguientes temas:

Crear un proyecto de OpenStack

Los proyectos son unidades organizativas en OpenStack. Pueden contener usuarios, instancias y otros objetos, como imágenes.

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.
2. En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.
3. Seleccione **Identidad > Proyectos** y haga clic en **Crear proyecto**.
4. En la pestaña **Información de proyecto**, introduzca un nombre y una descripción, y seleccione si desea habilitar el proyecto.
5. (opcional) En la pestaña **Miembros del proyecto**, agregue usuarios al proyecto.
6. (opcional) En la pestaña **Grupos del proyecto**, agregue grupos de usuarios al proyecto.
7. En la pestaña **Cuotas**, especifique las cuotas de recursos para el proyecto.
8. Haga clic en **Crear proyecto**.

El panel de control de VMware Integrated OpenStack asignará un identificador al nuevo proyecto y el proyecto se mostrará en la página **Proyectos**.

Nota El identificador de proyecto generado tiene una longitud de 32 caracteres. Sin embargo, cuando filtre por identificador de proyecto específico de la sección de grupo de seguridad en los registros del servidor de Neutron o en vRealize Log Insight, use únicamente los primeros 22 caracteres.

Pasos siguientes

En la columna **Acciones** ubicada a la derecha de cada proyecto, puede modificar la configuración del proyecto, lo cual incluye agregar y quitar usuarios y grupos, modificar cuotas de proyecto, y cambiar el nombre o el estado habilitado del proyecto.

Si deshabilita un proyecto, sus miembros no podrán acceder a él, pero sus instancias seguirán ejecutándose y se conservarán los datos del proyecto. Los usuarios asignados solo a proyectos deshabilitados no pueden iniciar sesión en el panel de control de VMware Integrated OpenStack.

Puede seleccionar uno o varios proyectos y hacer clic en **Eliminar proyectos** para quitarlos de forma permanente. No se pueden restaurar los proyectos eliminados.

Crear un usuario de nube

Los usuarios de nube tienen menos permisos que los administradores de nube. Los usuarios de nube pueden crear y administrar instancias, volúmenes, redes e imágenes para el proyecto al que están asignados.

Requisitos previos

Cree y habilite al menos un proyecto de OpenStack. Consulte Crear un proyecto de OpenStack.

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.
2. En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.
3. Seleccione **Identidad > Usuarios** y haga clic en **Crear usuario**.
4. Configure las opciones para el usuario.

Opción	Descripción
Nombre de usuario	Introduzca el nombre de usuario.
Descripción	(Opcional) Escriba una descripción para el usuario.
Correo electrónico	(Opcional) Escriba una dirección de correo electrónico para el usuario.
Contraseña/Confirmar contraseña	Cree una contraseña preliminar para el usuario. La contraseña puede cambiarse cuando el usuario inicie sesión por primera vez.
Proyecto principal	Seleccione el proyecto al que se asignará el usuario. Una cuenta de usuario debe asignarse a por lo menos un proyecto.

Opción	Descripción
Rol	Seleccione una función para el usuario. El usuario hereda los permisos asignados a la función especificada.
Habilitar	Seleccione **Habilitar** para permitir que el usuario inicie sesión y realice operaciones en OpenStack.

5 Haga clic en **Crear usuario**.

Pasos siguientes

En la columna **Acciones** ubicada a la derecha de cada usuario, puede modificar la configuración de usuario, cambiar la contraseña del usuario, y habilitar o deshabilitar el usuario.

Si desea asignar un solo usuario a varios proyectos, seleccione **Identidad > Proyectos** y haga clic en **Administrar miembros** junto al objeto que desee.

Puede crear un grupo que contenga varios usuarios para facilitar la administración. Consulte Crear un grupo de usuarios.

Puede seleccionar uno o varios usuarios y hacer clic en **Eliminar usuarios** para quitarlos de forma permanente. No se pueden restaurar los usuarios eliminados.

Crear un grupo de usuarios

Puede crear un grupo que contenga varios usuarios para facilitar la administración.

Requisitos previos

Cree los usuarios que desee. Consulte Crear un usuario de nube.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.

3 Seleccione **Identidad > Grupos** y haga clic en **Crear grupo**.

4 Escriba un nombre y una descripción, y haga clic en **Crear grupo**.

5 En la columna **Acciones** ubicada a la derecha del nuevo grupo, haga clic en **Administrar miembros**.

6 Haga clic en **Agregar usuarios**.

7 Seleccione uno o varios usuarios y haga clic en **Agregar usuarios**.

Pasos siguientes

Puede agregar el grupo de usuarios al crear o modificar un proyecto. Todos los usuarios del grupo heredarán las funciones especificadas en el proyecto del grupo.

Crear un grupo de seguridad del proveedor

Puede crear un grupo de seguridad del proveedor para bloquear el tráfico específico de un proyecto.

Los tenants crean y gestionan los grupos de seguridad estándares, mientras que el administrador de nube crea y gestiona los grupos de seguridad del proveedor. Los grupos de seguridad del proveedor tienen prioridad sobre los grupos de seguridad estándares y se aplican en todas las máquinas virtuales de un proyecto.

Para obtener instrucciones acerca de los grupos de seguridad estándares, consulte "Trabajar con grupos de seguridad" en la *Guía de usuario de VMware Integrated OpenStack*.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack.

2 Cree un grupo de seguridad del proveedor para un proyecto específico.

```
neutron security-group-create group-name --provider=True --tenant-id=project-id
```

3 Cree reglas para el grupo de seguridad del proveedor.

Nota Las reglas del grupo de seguridad del proveedor bloquean el tráfico especificado, mientras que las reglas de seguridad estándares permiten el tráfico especificado.

```
neutron security-group-rule-create group-name --tenant-id=project-id [--description rule-
description] [--direction {ingress | egress}] [--ethertype {IPv4 | IPv6}] [--protocol protocol] [--
port-range-min range-start --port-range-max range-end] [--remote-ip-prefix ip/prefix | --remote-
group-id remote-security-group]
```

Opción	Descripción
group-name	Introduzca el grupo de seguridad del proveedor que se creó en el paso 2.
--tenant-id	Introduzca el identificador del proyecto deseado.
--description	Introduzca una descripción personalizada de la regla.
--direction	Especifique **`ingress`** para bloquear el tráfico entrante o **`egress`** para bloquear el tráfico saliente. Si no se incluye este parámetro, se utiliza `ingress` de forma predeterminada.
--ethertype	Especifique **`IPv4`** o **`IPv6`**. Si no se incluye este parámetro, se utiliza `IPv4` de forma predeterminada.
--protocol	Especifique el protocolo que desea bloquear. Introduzca una representación con enteros comprendida entre 0 y 255, o uno de los siguientes valores: ■ **`icmp`** ■ **`icmpv6`** ■ **`tcp`** ■ **`udp`** Para bloquear todos los protocolos, no incluya este parámetro.

Opción	Descripción
--port-range-min	Introduzca el primer puerto que desea bloquear. Para bloquear todos los puertos, no incluya este parámetro. Para bloquear un solo puerto, introduzca el mismo valor para los parámetros `--port-range-min` y `--port-range-max`.
--port-range-max	Introduzca el último puerto que desea bloquear. Para bloquear todos los puertos, no incluya este parámetro. Para bloquear un solo puerto, introduzca el mismo valor para los parámetros `--port-range-min` y `--port-range-max`.
--remote-ip-prefix	Introduzca la red de origen del tráfico que desea bloquear (por ejemplo, 10.10.0.0/24). Este parámetro no se puede utilizar junto con el parámetro `--remote-group-id`.
--remote-group-id	Introduzca el nombre o el identificador del grupo de seguridad de origen del tráfico que desea bloquear. Este parámetro no se puede utilizar junto con el parámetro `--remote-ip-prefix`.

Las reglas del grupo de seguridad del proveedor se aplican en todos los puertos recién creados en las máquinas virtuales del proyecto especificado y no se pueden reemplazar con grupos de seguridad definidos por el tenant.

Pasos siguientes

Para aplicar uno o varios grupos de seguridad del proveedor en los puertos existentes, ejecute el siguiente comando:

```
neutron port-update port-id --provider-security-groups list=true group-id1...
```

Usar directivas de seguridad de NSX Data Center for vSphere en OpenStack

Puede aplicar directivas de seguridad de NSX Data Center for vSphere a través de grupos de seguridad de Neutron. También se puede usar esta función para insertar servicios de red de terceros.

Los grupos de seguridad estándar y de proveedor pueden emplear las directivas de seguridad de NSX Data Center for vSphere. Los grupos de seguridad estándar y de proveedor basados en reglas también pueden utilizarse junto con los grupos de seguridad basados en directivas de seguridad. Sin embargo, un grupo de seguridad asociado con una directiva de seguridad no puede contener reglas.

Las directivas de seguridad tienen prioridad sobre todas las reglas del grupo de seguridad. Si se aplica más de una directiva de seguridad en un puerto, el orden en el que se aplican las directivas se determina mediante NSX Data Center for vSphere. Puede cambiar el orden en vSphere Client en la página **Seguridad > Firewall**, en **Redes y seguridad**.

Requisitos previos

Cree las directivas de seguridad que desee en NSX Data Center for vSphere. Consulte "Crear una directiva de seguridad" en la *Guía de administración de NSX-T*.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

3. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
4. Quite la marca de comentario de los parámetros `nsxv_use_nsx_policies`, `nsxv_default_policy_id` y `nsxv_allow_tenant_rules_with_policy`, y configúrelos.

Opción	Descripción
nsxv_use_nsx_policies	Introduzca **`true`**.
nsxv_default_policy_id	Introduzca el identificador de la directiva de seguridad de NSX Data Center for vSphere que desea asociar con el grupo de seguridad predeterminado para los proyectos nuevos. Si no desea utilizar una directiva de seguridad de forma predeterminada, puede dejar que este parámetro siga siendo un comentario. Para encontrar el identificador de una directiva de seguridad, seleccione **Menú > Redes y seguridad** y haga clic en **Service Composer**. Abra la pestaña **Directivas de seguridad** y haga clic en el icono **Mostrar columnas** en la parte inferior izquierda de la tabla. Seleccione **Identificador del objeto** y haga clic en **Aceptar**. El identificador de cada directiva de seguridad se muestra en la tabla.
nsxv_allow_tenant_rules_with_policy	Escriba **`true`** para permitir que los tenants creen reglas y grupos de seguridad, o **`false`** para evitar que los tenants creen reglas o grupos de seguridad.

5. Implemente la configuración actualizada.

   ```
   sudo viocli deployment configure
   ```

   Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.
6. Inicie sesión en el nodo del controlador como `viouser`.
7. Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

   ```
   sudo su –
   source ~/cloudadmin.rc
   ```

8 Si desea utilizar grupos de seguridad adicionales con directivas de seguridad, puede llevar a cabo los siguientes pasos:

- Para asociar una directiva de seguridad de NSX Data Center for vSphere con un nuevo grupo de seguridad, cree el grupo y actualícelo con la directiva que desee:

```
neutron security-group-create security-group-name --tenant-id tenant-uuid
neutron security-group-update --policy=policy-id security-group-uuid
```

- Para migrar un grupo de seguridad existente a un grupo basado en directivas de seguridad, ejecute el siguiente comando:

```
sudo -u neutron nsxadmin -r security-groups -o migrate-to-policy --property policy-id=policy-
id --property security-group-id=security-group-uuid
```

Nota Este comando quita todas las reglas del grupo de seguridad especificado. Asegúrese de que la directiva de destino está configurada de manera tal que no se interrumpirá la conexión de red.

9 Configure Neutron para dar prioridad a las directivas de seguridad de NSX Data Center for vSphere a través de los grupos de seguridad.

```
sudo -u neutron nsxadmin --config-file /etc/neutron/neutron.conf --config-
file /etc/neutron/plugins/vmware/nsxv.ini -r firewall-sections -o nsx-reorder
```

Instancias de OpenStack

6

Las instancias son máquinas virtuales que se ejecutan en la nube.

Puede administrar instancias para usuarios en varios proyectos. Este usuario puede ver, cerrar, editar y migrar instancias, así como ejecutar el reinicio parcial o completo de una instancia, y crear una instantánea a partir de una instancia. También puede ver los registros de las instancias o iniciar una consola de VNC para una instancia.

Este capítulo incluye los siguientes temas:

Importar máquinas virtuales en VMware Integrated OpenStack con NSX Data Center for vSphere

Puede importar máquinas virtuales desde vSphere en la implementación de VMware Integrated OpenStack y administrarlas como instancias de OpenStack.

Este procedimiento se aplica a las implementaciones con redes de NSX Data Center for vSphere o VDS. Para las implementaciones de NSX-T Data Center, consulte Importar máquinas virtuales en VMware Integrated OpenStack con NSX-T Data Center.

Las máquinas virtuales importadas se convierten en instancias de OpenStack, pero siguen siendo distintas.

- Si una máquina virtual tiene varios discos, los discos se importan como volúmenes de Cinder.
- Las redes existentes se importan como redes de proveedor del tipo `portgroup` con acceso restringido al arrendatario determinado.
- Después de importar una máquina virtual con un respaldo de red específico, ya no se puede importar la misma red en otro proyecto.
- Las subredes de Neutron se crean automáticamente con DHCP deshabilitado.
- Los puertos de Neutron se crean de manera automática en función de las direcciones IP y MAC de la tarjeta de interfaz de red en la máquina virtual.

Nota Si el servidor DHCP no puede mantener la misma dirección IP durante la renovación de la concesión, se mostrará la dirección IP incorrecta en la información de la instancia en OpenStack. Para evitar este problema, utilice los enlaces de DHCP estáticos en los servidores DHCP existentes y no ejecute nuevas instancias de OpenStack en redes importadas.

Las máquinas virtuales se importan mediante Data Center Command-Line Interface (DCLI) en Servidor de administración de OpenStack.

Requisitos previos

Compruebe que las máquinas virtuales que desea importar están en la misma instancia de vCenter Server.

Procedimiento

1. En vSphere, agregue los clústeres que contengan las máquinas virtuales deseadas como clústeres de proceso en la implementación de VMware Integrated OpenStack. Para obtener instrucciones, consulte Agregar clústeres de proceso a una implementación de OpenStack.
2. Inicie sesión en Servidor de administración de OpenStack como `viouser`.

3 Si desea impedir que se cambien el nombre o la ubicación de las máquinas virtuales importadas, actualice la configuración de implementación.

a Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

```
sudo mkdir -p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

b Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

c Quite la marca de comentario del parámetro `nova_import_vm_relocate` y establezca su valor como `false`.

d Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

4 Conéctese al endpoint de vAPI de VMware Integrated OpenStack.

```
dcli +server https://mgmt-server-ip:9449/api +i
```

Si no se puede conectar al servidor, consulte DCLI no se puede conectar al servidor.

5 Importe máquinas virtuales sin administrar en VMware Integrated OpenStack.

Nota Cuando se ejecuta un comando, DCLI le solicita que introduzca las credenciales de administrador para la instancia de vCenter Server. Puede guardar estas credenciales para no tener que introducir el nombre de usuario y la contraseña cada vez.

- Ejecute el siguiente comando para importar todas las máquinas virtuales sin administrar:

```
com vmware vio vm unmanaged importall --cluster cluster-name [--tenant-mapping {FOLDER |
RESOURCE_POOL} [--root-folder root-folder | --root-resource-pool root-resource-pool]]
```

Opción	Descripción
`--cluster`	Introduzca el clúster de proceso que contiene las máquinas virtuales que desea importar.
`--tenant-mapping {FOLDER | RESOURCE_POOL}`	Especifique si desea asignar las máquinas virtuales importadas a los proyectos de OpenStack en función de su ubicación en carpetas o grupos de recursos. Si no incluye este parámetro, todas las máquinas virtuales importadas se convertirán en instancias en el proyecto **import_service** de forma predeterminada.

Opción	Descripción
`--root-folder ROOT_FOLDER`	Si especificó **`FOLDER`** para el parámetro `--tenant-mapping`, puede proporcionar el nombre de la carpeta raíz que contiene las máquinas virtuales que se van a importar. Todas las máquinas virtuales de la carpeta especificada o cualquiera de sus subcarpetas se importarán como instancias en un proyecto de OpenStack con el mismo nombre que la carpeta en la que se encuentran. **Nota** Si especifica `--tenant-mapping FOLDER`, pero no especifica `--root-folder`, el nombre de la carpeta de nivel superior del clúster se utiliza de manera predeterminada.
`--root-resource-pool ROOT_RESOURCE_POOL`	Si especificó **`RESOURCE_POOL`** para el parámetro `--tenant-mapping`, puede proporcionar el nombre del grupo de recursos raíz que contiene las máquinas virtuales que se van a importar. Todas las máquinas virtuales en el grupo de recursos especificado o cualquiera de sus grupos de recursos secundarios se importarán como instancias en un proyecto de OpenStack con el mismo nombre que el grupo de recursos en el que se encuentran.

- Ejecute el siguiente comando para importar una máquina virtual determinada:

```
com vmware vio vm unmanaged importvm --vm vm-id [--tenant project-name] [--nic-mac-address nic-mac --nic-ipv4-address nic-ip] [--root-disk root-disk-path] [--nics specifications]
```

Opción	Descripción
`--vm`	Introduzca el identificador de la máquina virtual que desee importar. Puede ver los valores de identificador de todas las máquinas virtuales sin administrar. Para ello, ejecute el comando `com vmware vio vm unmanaged list`.
`--tenant`	Especifique el proyecto de OpenStack en el que desea importar la máquina virtual. Si no incluye este parámetro, se utiliza el proyecto `import_service` de forma predeterminada.
`--nic-mac-address`	Introduzca la dirección MAC de la tarjeta de interfaz de red en la máquina virtual. Si no incluye este parámetro, el proceso de importación intenta detectar las direcciones MAC e IP automáticamente. **Nota** Si incluye este parámetro, también debe incluir el parámetro `nic_ipv4_address`.
`--nic-ipv4-address`	Introduzca la dirección IP y el prefijo de la tarjeta de interfaz de red en la máquina virtual. Introduzca el valor en notación CIDR (por ejemplo, 10.10.1.1/24). Este parámetro debe utilizarse junto con el parámetro `--nic-mac-address`.
`--root-disk`	Para una máquina virtual con varios discos, especifique la ruta de acceso del almacén de datos del disco raíz con el siguiente formato: **`--root-disk '[datastore1] foo/foo_1.vmdk'`**
`--nics`	Para una máquina virtual con varias NIC, especifique las direcciones MAC e IP de cada NIC con el formato JSON. Utilice los siguientes pares clave-valor: ■ mac_address: dirección MAC de la NIC con formato estándar. ■ ipv4_address: dirección IPv4 en notación CIDR. Por ejemplo: `--nics '[{"mac_address": "00:50:56:9a:f5:7b", "ipv4_address": "10.10.1.1/24"}, {"mac_address": "00:50:56:9a:ee:be", "ipv4_address": "10.10.2.1/24"}]'`

Importar máquinas virtuales en VMware Integrated OpenStack con NSX-T Data Center

Puede importar máquinas virtuales desde vSphere en la implementación de VMware Integrated OpenStack y administrarlas como instancias de OpenStack.

Importante Este procedimiento solamente se admite en VMware Integrated OpenStack 5.1.0.1 y versiones posteriores.

Este procedimiento se aplica a implementaciones con redes de NSX-T Data Center. Para implementaciones de VDS o NSX Data Center for vSphere, consulte Importar máquinas virtuales en VMware Integrated OpenStack con NSX Data Center for vSphere.

Las máquinas virtuales importadas se convierten en instancias de OpenStack, pero siguen siendo distintas.

- Si una máquina virtual tiene varios discos, los discos se importan como volúmenes de Cinder.
- Después de importar una máquina virtual con un respaldo de red específico, ya no se puede importar la misma red en otro proyecto. Si desea utilizar una red para varios proyectos, configúrela como una red compartida.

Las máquinas virtuales se importan mediante Data Center Command-Line Interface (DCLI) en Servidor de administración de OpenStack.

Requisitos previos

Compruebe que las máquinas virtuales que desea importar están en la misma instancia de vCenter Server.

Procedimiento

1. En vSphere, agregue el clúster que contiene la máquina virtual que desee como un clúster de proceso en la implementación de VMware Integrated OpenStack. Para obtener instrucciones, consulte Agregar clústeres de proceso a una implementación de OpenStack.
2. Conecte la máquina virtual a una red de Neutron.

   Puede utilizar una red de proveedores o una red de tenants para realizar este procedimiento.

   a. En vSphere Client, abra la vista **Hosts y clústeres**.

   b. Haga clic con el botón secundario en cada máquina virtual que desee importar y seleccione **Editar configuración...**.

   c. En la lista desplegable junto al adaptador de red, seleccione la red de Neutron que desea utilizar.

   d. Expanda la configuración del adaptador de red y registre su dirección MAC.

3 Cree una red opaca temporal para la máquina virtual.

   a En NSX Manager, seleccione **Conmutación > Conmutadores** y haga clic en **Agregar**.

   b Introduzca un nombre para el conmutador y seleccione la zona de transporte superpuesta.

   c Haga clic en **Agregar**.

   d En la columna **Conmutador lógico**, haga clic en el nombre del conmutador que creó.

   e Registre el identificador del conmutador, tal y como se muestra en la columna **Descripción general**.

4 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

5 Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

6 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

7 Quite el comentario del parámetro `nova_import_net_id` y establezca su valor en el identificador del conmutador que creó en el paso 3.

8 Si desea evitar que las máquinas virtuales importadas cambien de nombre o de ubicación, quite el comentario del parámetro `nova_import_vm_relocate` y establezca su valor en `false`.

9 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

   Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

10 Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su –
source ~/cloudadmin.rc
```

11 Cree un puerto de Neutron que utilice la dirección MAC del adaptador de red de la máquina virtual.

```
neutron port-create network --name port --tenant-id project-id --mac-address vm-mac [--fixed-ip
ip_address=vm-ip]
```

Opción	Descripción
network	Introduzca el nombre de la red de Neutron a la que conectó la máquina virtual.
--name	Introduzca un nombre para el puerto.
--tenant-id	Especifique el UUID del proyecto para el que se va a crear el puerto.

Opción	Descripción
--mac-address	Introduzca la dirección MAC del adaptador de red de la máquina virtual que registró en el paso 2d.
--fixed-ip	Introduzca la dirección IP de la máquina virtual. Si la máquina virtual no tiene una dirección IP o si no desea conservar la dirección IP existente, puede omitir este parámetro.

12 Conéctese al endpoint de vAPI de VMware Integrated OpenStack.

```
dcli +server https://mgmt-server-ip:9449/api +i
```

Si no se puede conectar al servidor, consulte DCLI no se puede conectar al servidor.

13 Importe la máquina virtual en VMware Integrated OpenStack.

```
com vmware vio vm unmanaged importvm --vm vm-moid --nic-net-id network-uuid --nic-port-id port-uuid [--tenant project-name] [--root-disk root-disk-path]
```

Opción	Descripción
--vm	Introduzca el identificador de objeto administrado (Managed Object Identifier, MOID) de la máquina virtual que desea importar. Puede ver los identificadores MOID de todas las máquinas virtuales sin administrar. Para ello, ejecute el comando `com vmware vio vm unmanaged list`.
--nic-net-id	Introduzca el UUID de la red de Neutron a la que conectó la máquina virtual.
--nic-port-id	Introduzca el UUID del puerto que creó para la máquina virtual.
--tenant	Especifique el proyecto de OpenStack en el que desea importar la máquina virtual. Si no incluye este parámetro, se utiliza el proyecto `import_service` de forma predeterminada.
--root-disk	Para una máquina virtual con varios discos, especifique la ruta de acceso del almacén de datos del disco raíz con el siguiente formato: **`--root-disk '[datastore1] foo/foo_1.vmdk'`**

Nota Cuando se ejecuta un comando, DCLI le solicita que introduzca las credenciales de administrador para la instancia de vCenter Server. Puede guardar estas credenciales para no tener que introducir el nombre de usuario y la contraseña cada vez.

Controlar el estado de una instancia

Como usuario administrativo de la nube, puede pausar, cancelar la pausa, suspender, reanudar, reiniciar en caliente o en frío, o finalizar una instancia.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione un proyecto de administración.

3 Seleccione **Administrador > Panel de sistema > Instancias**.

4 Seleccione la instancia cuyo estado desea administrar.

5 En la columna Acciones, haga clic en **Más** y seleccione el estado en el menú desplegable.

Los elementos que aparecen en texto rojo están deshabilitados.

Realizar un seguimiento del uso de las instancias

Es posible realizar un seguimiento del uso de las instancias para cada proyecto. Se puede realizar un seguimiento de los costos mensuales con métricas como cantidad de VCPU, discos, RAM y tiempo de actividad de todas las instancias.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione un proyecto de administración.

3 Seleccione **Administrador > Panel de sistema > Descripción general**.

La página Descripción general muestra el resumen de uso y la información de uso específica del proyecto. Se puede especificar un período para mostrar la información de uso. También se puede descargar un resumen en formato CSV.

4 (opcional) Especifique un período para la generación del informe y haga clic en **Enviar**.

5 (opcional) Haga clic en **Descargar resumen en formato CSV** para descargar un informe de uso.

Migrar una instancia

Puede migrar en vivo una instancia de OpenStack a un nodo informático diferente.

Nota Las instancias administradas por VMware Integrated OpenStack deben migrarse mediante los comandos de OpenStack. No utilice vCenter Server u otros métodos para migrar instancias de OpenStack.

Requisitos previos

- Los nodos informáticos de origen y de destino deben estar ubicados en la misma instancia de vCenter Server.
- Los nodos informáticos de origen y de destino deben tener al menos un conmutador distribuido en común. Si dos conmutadores distribuidos están conectados al nodo informático de origen, pero solo hay un conmutador distribuido asociado al nodo informático de destino, la migración en vivo se realizará correctamente, pero la instancia de OpenStack se conectará solo al grupo de puertos del conmutador distribuido que sea común en los dos nodos informáticos.

- Si desea migrar en vivo una instancia con una unidad de CD-ROM conectada, compruebe que el entorno tiene un almacén de datos compartido al que puedan acceder todos los hosts.

  Importante La migración en vivo de una instancia con una unidad de CD-ROM conectada solamente se admite en VMware Integrated OpenStack 5.1.0.1 o versiones posteriores.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Si la instancia tiene una unidad de CD-ROM conectada, configure un almacén de datos compartido para la migración de CD-ROM.
   a. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

   b. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
   c. Quite el comentario del parámetro `nova_shared_datastore_regex` y establezca su valor en el nombre del almacén de datos compartido en vSphere.
   d. Implemente la configuración actualizada.

   ```
   sudo viocli deployment configure
   ```

   Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.
3. Inicie sesión en el nodo del controlador como `viouser`.
4. Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

   ```
   sudo su –
   source ~/cloudadmin.rc
   ```

5. Migre la instancia al nodo informático deseado.

   ```
   openstack server migrate compute–name instance–uuid ––live
   ```

   - Para buscar el nombre de un nodo informático, ejecute el comando `openstack host list` y vea la columna **Nombre de host**.
   - Para encontrar el UUID de la instancia, ejecute el comando `openstack server list` y vea la columna **ID**.

Pasos siguientes

Puede ejecutar el comando `openstack server show` *`instance–uuid`* para confirmar que la instancia se ha migrado al nodo informático deseado.

Habilitar cambio de tamaño en estado activo

Puede habilitar el cambio de tamaño en estado activo para las instancias de OpenStack mediante la configuración de los metadatos de imagen. Con el cambio de tamaño en estado activo, puede cambiar el tamaño de disco, la memoria y las vCPU de una instancia mientras está encendida.

Nota No se puede reiniciar una instancia habilitada para el cambio de tamaño en estado activo que tenga un volumen asociado. Si necesita reiniciar la instancia, primero desasocie el volumen.

Requisitos previos

- No cree instancias habilitadas para cambiar el tamaño en estado activo mediante puertos habilitados para SR-IOV. El cambio de tamaño en estado activo no es compatible con SR-IOV.
- No utilice instancias habilitadas para cambiar el tamaño en estado activo en centros de datos virtuales de tenant. El cambio de tamaño en estado activo no es compatible con los centros de datos virtuales de tenant.

Adicionalmente, se aplican las siguientes condiciones para cambiar el tamaño del disco en estado activo:

- Utilice VMDK como formato de disco de la imagen.
- Utilice un tipo de adaptador de disco virtual de SCSI para la imagen. No se admiten los tipos de adaptador IDE.
- Implemente máquinas virtuales a partir de la imagen como clones completos. No se puede cambiar el tamaño de clones vinculados en estado activo.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su -
source ~/cloudadmin.rc
```

3 Cree una nueva imagen que esté habilitada para el cambio de tamaño en estado activo.

```
openstack image create image-name --disk-format {vmdk | iso} --container-format bare --file image-
file {--public | --private} [--property vmware_adaptertype="vmdk-adapter-type"] [--property
vmware_disktype="{sparse | preallocated | streamOptimized}"] --property vmware_ostype="operating-
system" --property img_linked_clone="false" --property os_live_resize="{vcpu | memory | disk}"
```

Opción	Descripción
image-name	Introduzca el nombre de la imagen de origen.
--disk-format	Introduzca **`vmdk`**.
--container-format	Introduzca **`bare`**. Actualmente, Glance no utiliza el argumento de formato de contenedor.
--file	Especifique el archivo de imagen que va a cargar.

Opción	Descripción
{--public | --private}	Incluya `--public` para que la imagen esté disponible para todos los usuarios o `--private` para que la imagen esté disponible únicamente para el usuario actual.
--property vmware_adaptertype	Especifique el tipo de adaptador del disco VMDK. Para cambiar el tamaño del disco en estado activo, debe especificar un adaptador SCSI. Si no incluye este parámetro, el tipo de adaptador se determina por introspección.
--property vmware_disktype	Especifique **`sparse`**, **`preallocated`** o **`streamOptimized`**. Si no incluye este parámetro, el tipo de disco se determina por introspección.
--property vmware_ostype	Especifique el sistema operativo en la imagen.
--property img_linked_clone	Introduzca **`false`**.
--property os_live_resize	Especifique **`vcpu`**, **`memory`**, **`disk`** o cualquier combinación separada por comas (por ejemplo, **`vcpu,memory,disk`**).

Cuando se crean máquinas virtuales con la imagen que se definió en este procedimiento, se puede cambiar el tamaño de dichas máquinas virtuales sin tener que apagarlas.

Habilitar la compatibilidad de página gigante

Para proporcionar mejoras de rendimiento importantes o necesarias para algunas cargas de trabajo, puede habilitar la compatibilidad de página gigante de OpenStack hasta 1 GB por página. Las páginas gigantes se solicitan explícitamente mediante el uso de especificaciones adicionales de tipo o metadatos de imagen.

Requisitos previos

- Compruebe que se esté ejecutando VMware Integrated OpenStack 5.0 o posterior.
- Compruebe que su implementación incluye vSphere 6.7 o posterior.

Procedimiento

1 Agregue una especificación adicional de tipo para solicitar páginas gigantes con las propiedades `hw` y `quota`.

```
$ openstack flavor set m1.large --property hw:mem_page_size=large
$ openstack flavor set m1.large --property quota:memory_reservation_percent=100
```

2 Cree una instancia de OpenStack con el tipo de página gigante, como en el ejemplo siguiente.

```
$ openstack server create --flavor m1.large --image ubuntu foobar
```

3 Inicie sesión en el sistema operativo invitado en la consola de VMware Integrated OpenStack.

El modo de habilitar páginas gigantes es diferente para cada sistema operativo. El siguiente ejemplo muestra cómo habilitar páginas gigantes persistentes en un host Linux.

a Para asignar páginas gigantes en tiempo de ejecución, modifique `/etc/default/grub` para que incluya algunos parámetros de página gigante.

```
echo 'GRUB_CMDLINE_LINUX="default_hugepagesz=1G hugepagesz=1G hugepages=2
transparent_hugepage=never"' > /etc/default/grub
```

b Actualice el cargador de arranque.

```
update-grub2
```

c Reinicie la instancia.

d Compruebe que la instancia utilice páginas gigantes.

```
grep "Huge" /proc/meminfo
```

El valor de `Hugepagesize` debe ser 1 GB o menos.

Usar afinidad para controlar la colocación de instancias de OpenStack

Puede colocar las instancias mediante grupos de servidores de OpenStack con una directiva de afinidad o antiafinidad. Afinidad indica que debe colocar todas las instancias en el grupo en el mismo host, y antiafinidad indica que no se pueden colocar instancias del grupo en el mismo host.

Las directivas de afinidad y antiafinidad no pueden determinar el host ESXi específico en el que se colocan las instancias. Estas directivas solo controlan si las instancias se colocan en los mismos hosts que otras instancias de un grupo de servidores. Para colocar instancias en hosts específicos, consulte Usar DRS para controlar la colocación de instancias de OpenStack.

Requisitos previos

Compruebe que la configuración del filtro deseada no entre en conflicto con ninguna configuración administrativa existente, como reglas de DRS que administran la colocación de instancias en hosts.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su -
source ~/cloudadmin.rc
```

3 Cree un grupo de servidores con la directiva que desee.

```
openstack server group create group-name --policy {affinity | anti-affinity}
```

Opción	Descripción
group-name	Introduzca un nombre para el grupo de servidores.
--policy	Introduzca **affinity** para colocar instancias en el mismo host o **anti-affinity** para impedir que las instancias se coloquen en el mismo host.

4 Al iniciar una instancia, pase el grupo de servidores como una sugerencia de programador para implementar la afinidad o la antiafinidad.

```
openstack server create instance-name --image image-uuid --flavor flavor-name --nic net-id=network-uuid --hint group=servergroup-uuid
```

Pasos siguientes

Confirme que las reglas de afinidad y las instancias están configuradas correctamente. En vCenter Server, seleccione el clúster de proceso, abra la pestaña **Configurar** y haga clic en **Reglas de host/máquina virtual**.

Usar DRS para controlar la colocación de instancias de OpenStack

Es posible usar la configuración de DRS de vSphere para controlar la manera en que se colocan las instancias de OpenStack específicas en los hosts del clúster de proceso. Después de configurar DRS, también se pueden modificar los metadatos de las imágenes de origen en OpenStack para garantizar que las instancias generadas a partir de esas imágenes se identifiquen correctamente para su colocación.

Procedimiento

1 Definir grupos de máquinas virtuales y hosts para colocar instancias de OpenStack

Se definen grupos de máquinas virtuales y de hosts para que contengan y administren instancias de OpenStack específicas.

2 Crear una regla de DRS para colocación de instancias de OpenStack

Las reglas de DRS se crean para administrar la distribución de instancias de OpenStack en un grupo de máquinas virtuales a un grupo de hosts específico.

3 Aplicar configuración de grupo de máquinas virtuales a metadatos de imagen

Se modifican los metadatos de una imagen de origen para colocar automáticamente instancias en grupos de máquinas virtuales. A continuación, las reglas de DRS determinan los grupos de host en los que se crearán estas instancias.

Definir grupos de máquinas virtuales y hosts para colocar instancias de OpenStack

Se definen grupos de máquinas virtuales y de hosts para que contengan y administren instancias de OpenStack específicas.

Requisitos previos

- Asegúrese de que el clúster de proceso contiene al menos una máquina virtual. Si el clúster de proceso no contiene ninguna máquina virtual, cree una máquina virtual ficticia para realizar este procedimiento.
- En el clúster de proceso, habilite DRS y establezca **Automatización de DRS** como **Parcialmente automatizado** o **Totalmente automatizado**.
- En el clúster de proceso, establezca **Administración de energía** como **Desactivado**.

Procedimiento

1. En vSphere Client, seleccione el clúster de proceso y haga clic en **Configurar**.
2. En **Configuración**, haga clic en **Grupos de hosts/máquinas virtuales**.
3. Cree un grupo de máquinas virtuales.
   a. Haga clic en **Agregar**.
   b. Introduzca un nombre y seleccione **Grupo de máquinas virtuales** del menú desplegable **Tipo**.
   c. Haga clic en **Agregar**.
   d. En la pestaña **Filtrar**, seleccione máquinas virtuales para agregarlas al grupo.
   e. Haga clic en **Aceptar**.
4. Cree un grupo de hosts.
   a. Haga clic en **Agregar**.
   b. Introduzca un nombre y seleccione **Grupo de hosts** del menú desplegable **Tipo**.
   c. Haga clic en **Agregar**.
   d. En la pestaña **Filtrar**, seleccione hosts para agregarlos al grupo.
   e. Haga clic en **Aceptar**.

Pasos siguientes

Cree una regla que determine cómo se distribuyen las instancias de OpenStack asignadas al grupo de máquinas virtuales en los hosts del grupo de hosts.

Crear una regla de DRS para colocación de instancias de OpenStack

Las reglas de DRS se crean para administrar la distribución de instancias de OpenStack en un grupo de máquinas virtuales a un grupo de hosts específico.

Requisitos previos

- Defina al menos un grupo de máquinas virtuales y al menos un grupo de hosts. Consulte Definir grupos de máquinas virtuales y hosts para colocar instancias de OpenStack.
- En el clúster de proceso, habilite DRS y establezca **Automatización de DRS** como **Parcialmente automatizado** o **Totalmente automatizado**.
- En el clúster de proceso, establezca **Administración de energía** como **Desactivado**.

Procedimiento

1. En vSphere Client, haga clic en el clúster de proceso y seleccione **Configurar**.
2. En **Configuración**, haga clic en **Reglas de host/máquina virtual**.
3. Haga clic en el botón **Agregar...**.
4. Introduzca un nombre para la regla y seleccione la opción **Habilitar regla**.
5. En el menú desplegable **Tipo**, seleccione **Máquinas virtuales a hosts**.
6. En el menú desplegable **Grupo de máquinas virtuales**, seleccione el grupo de máquinas virtuales que contenga las instancias de OpenStack que desea colocar.
7. En el siguiente menú desplegable, seleccione una especificación para la regla.

Opción	Descripción
Debe ejecutarse en los hosts del grupo.	Las instancias de OpenStack del grupo de máquinas virtuales especificado deben ejecutarse en los hosts del grupo de hosts especificado.
Debería ejecutarse en los hosts del grupo.	Las instancias de OpenStack del grupo de máquinas virtuales especificado deberían, pero no están obligadas a, ejecutarse en los hosts del grupo de hosts especificado.
No debe ejecutarse en los hosts del grupo.	Las instancias de OpenStack del grupo de máquinas virtuales especificado nunca deben ejecutarse en los hosts del grupo de hosts especificado.
No debería ejecutarse en los hosts del grupo.	Las instancias de OpenStack del grupo de máquinas virtuales especificado no deben, pero pueden, ejecutarse en los hosts del grupo de hosts especificado.

8. En el menú desplegable **Grupo de hosts**, seleccione el grupo de hosts que contenga los hosts en los que se colocarán las instancias de OpenStack y haga clic en **Aceptar**.

Pasos siguientes

En el panel de control de VMware Integrated OpenStack, modifique los metadatos de una imagen específica para asegurarse de que todas las instancias generadas a partir de esa imagen se incluyan automáticamente en el grupo de máquinas virtuales y, por tanto, estén sujetas a la regla de DRS.

Aplicar configuración de grupo de máquinas virtuales a metadatos de imagen

Se modifican los metadatos de una imagen de origen para colocar automáticamente instancias en grupos de máquinas virtuales. A continuación, las reglas de DRS determinan los grupos de host en los que se crearán estas instancias.

Requisitos previos

Configure un grupo de máquinas virtuales y un grupo de hosts para el clúster de proceso.

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.
2. En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.
3. Seleccione **Administrador > Proceso > Imágenes**.
4. Cree una nueva imagen o elija una imagen existente.
5. Haga clic en la flecha abajo que aparece junto al tipo que desea utilizar y seleccione **Actualizar metadatos**.
6. En el panel **Metadatos disponibles**, expanda **Opciones de controlador de VMware** y haga clic en el icono **Agregar** (signo más) que aparece junto al **grupo de máquinas virtuales de DRS**.
7. Introduzca el nombre del grupo de máquinas virtuales que desee como el valor del parámetro `vmware_vm_group` y haga clic en **Guardar**.

Todas las instancias de OpenStack generadas a partir de esta imagen de origen se asignarán automáticamente al grupo de máquinas virtuales especificado y las regirán sus reglas de DRS.

Configurar la asignación de recursos de QoS para instancias mediante metadatos de tipo

Puede controlar las asignaciones de recursos de QoS, como límites, reservas y recursos compartidos, para CPU, RAM, IOPS de disco e interfaz de red virtual (VIF) si modifica los metadatos del tipo utilizado para crear la instancia. Todas las instancias creadas posteriormente mediante ese tipo heredarán la configuración de metadatos.

La asignación de recursos de QoS también puede especificarse a través de metadatos de imagen. Si se produce un conflicto, la configuración de metadatos de imagen anula la configuración de metadatos de tipo. Consulte Configurar la asignación de recursos de QoS para instancias mediante metadatos de imagen.

Requisitos previos

- Requiere VMware Integrated OpenStack versión 2.0.x o posterior.
- Requiere vSphere versión 6.0 o posterior.

- Compruebe que VMware Integrated OpenStack se esté ejecutando en vSphere.
- Compruebe si se encuentra conectado al panel de control de VMware Integrated OpenStack como administrador de nube.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione un proyecto de administración.

3 Seleccione **Administrador > Sistema > Tipos**.

4 (opcional) Cree un tipo específico para establecer las asignaciones de recursos de QoS.

Debe crear un tipo personalizado para que contenga la configuración específica. Esto deja la configuración de tipo original intacta y disponible para otros usuarios.

5 Seleccione el tipo que desea modificar.

6 En la columna Acciones de la lista de imágenes, haga clic en la flecha hacia abajo y seleccione **Actualizar metadatos**.

7 En la columna debajo de Metadatos disponibles, expanda la pestaña **Cuota de VMware**.

Nota Si la pestaña Cuota de VMware no aparece, es posible que las propiedades de metadatos relacionadas ya estén configuradas.

8 Haga clic en el signo más (**+**) junto a la propiedad de metadatos de Cuota de VMware que desee agregar.

Sugerencia Para agregar todas las opciones a la vez, haga clic en el signo más (**+**) en la pestaña Cuota de VMware.

En la columna debajo de Metadatos existentes, aparecen las propiedades de metadatos recién agregadas.

9 Configure las propiedades de metadatos.

Propiedad de metadatos	Descripción
Cuota: límite de CPU	Aplica la propiedad de metadatos `quota:cpu_limit`. Especifica el límite superior para la asignación de CPU en MHz. Este parámetro garantiza que la instancia nunca use más que la cantidad definida de asignación de CPU. Escriba **0** para que la asignación de CPU sea ilimitada.
Cuota: reserva de CPU	Aplica la propiedad de metadatos `quota:cpu_reservation`. Especifica el mínimo de CPU de reserva garantizado en MHz. Este parámetro garantiza que la instancia tenga la cantidad reservada de ciclos de CPU disponible durante la contención de recursos.

Propiedad de metadatos	Descripción
Cuota: nivel de recursos compartidos de CPU	Aplica la propiedad de metadatos `quota:cpu_shares_level`. Especifica el nivel de recursos compartidos que se asigna al valor numérico predefinido de recursos compartidos. Si selecciona el nivel **`custom`**, debe incluir la propiedad de metadatos `quota:cpu_shares_value`. Vea Cuota: valor de recursos compartidos de CPU a continuación.
Cuota: valor de recursos compartidos de CPU	Aplica la propiedad de metadatos `quota:cpu_shares_value`. Especifica el número de recursos compartidos asignados a la instancia. Aplique esta propiedad solo si establece la propiedad de metadatos `quota:cpu_shares_level` como **`custom`**. De lo contrario, esta propiedad se ignorará.
Cuota: límite de E/S de disco	Aplica la propiedad de metadatos `quota:disk_io_limit`. Especifica el límite superior en segundos para las transacciones de disco en operaciones de E/S por segundo (IOPS). Este parámetro garantiza que la instancia nunca use más que la cantidad de IOPS de disco definida y puede usarse para aplicar un límite al rendimiento del disco de la instancia. Escriba **`0`** para que la cantidad de IOPS sea ilimitada.
Cuota: reserva de E/S de disco	Aplica la propiedad de metadatos `quota:disk_io_reservation`. Especifica el mínimo garantizado en segundos para las transacciones de disco en operaciones de E/S por segundo (IOPS). Este parámetro garantiza que la instancia reciba la cantidad reservada de IOPS de disco durante la contención de recursos.
Cuota: nivel de recursos compartidos de E/S de disco	Aplica la propiedad de metadatos `quota:disk_io_shares_level`. Especifica el nivel de recursos compartidos que se asigna al valor numérico predefinido de recursos compartidos. Si selecciona el nivel **`custom`**, debe incluir la propiedad de metadatos `quota:disk_io_shares_share` (Cuota: valor de recursos compartidos de E/S de disco).
Cuota: valor de recursos compartidos de E/S de disco	Aplica la propiedad de metadatos `quota:disk_io_shares_share`. Especifica el número de recursos compartidos asignados a la instancia. Aplique esta propiedad solo si establece la propiedad de metadatos `quota:disk_io_shares_level` como **`custom`**. De lo contrario, esta propiedad se ignorará.
Cuota: límite de memoria	Aplica la propiedad de metadatos `quota:memory_limit`. Especifica el límite superior para la asignación de memoria en MB. Este parámetro garantiza que la instancia nunca use más que la cantidad definida de memoria. Escriba **`0`** para que la asignación de memoria sea ilimitada.
Cuota: reserva de memoria	Aplica la propiedad de metadatos `quota:memory_reservation`. Especifica el mínimo garantizado de reserva de memoria en MB. Este parámetro garantiza que la instancia reciba la cantidad reservada de memoria durante la contención de recursos.
Cuota: nivel de recursos compartidos de memoria	Aplica la propiedad de metadatos `quota:memory_shares_level`. Especifica el nivel de recursos compartidos que se asigna al valor numérico predefinido de recursos compartidos. Si selecciona el nivel **`custom`**, debe incluir la propiedad de metadatos `quota:memory_shares_share` (Cuota: valor de recursos compartidos de memoria).

Propiedad de metadatos	Descripción
Cuota: valor de recursos compartidos de memoria	Aplica la propiedad de metadatos `quota:memory_shares_share`. Especifica el número de recursos compartidos asignados a la instancia. Aplique esta propiedad solo si establece la propiedad de metadatos `quota:memory_shares_level` como **`custom`**. De lo contrario, esta propiedad se ignorará.
Cuota: límite de VIF	Aplica la propiedad de metadatos `quota:vif_limit`. Especifica el límite superior para el ancho de banda VIF en Mbps. Este parámetro garantiza que VIF nunca use más que la cantidad definida de ancho de banda. Escriba **`0`** para que la asignación de ancho de banda sea ilimitada.
Cuota: reserva de VIF	Aplica la propiedad de metadatos `quota:vif_reservation`. Especifica el mínimo garantizado de ancho de banda para VIF en Mbps. Este parámetro garantiza que el adaptador virtual de la instancia obtenga la cantidad reservada de ancho de banda durante la contención de recursos. Si la instancia usa menos que la cantidad reservada, el resto queda disponible para otros adaptadores virtuales.
Cuota: nivel de recursos compartidos de VIF	Aplica la propiedad de metadatos `quota:vif_shares_level`. Especifica el nivel de recursos compartidos que se asigna al valor numérico predefinido de recursos compartidos. Si selecciona el nivel **`custom`**, debe incluir la propiedad de metadatos `quota:vif_shares_share` (Cuota: valor de recursos compartidos de VIF).
Cuota: valor de recursos compartidos de VIF	Aplica la propiedad de metadatos `quota:vif_shares_share`. Si se usa 'custom', este será el número de recursos compartidos.

10 Haga clic en **Guardar**.

Ahora los metadatos de tipo están configurados para límites, reservas y recursos compartidos de CPU, IOPS, memoria y ancho de banda de red. Esta configuración se aplicará a todas las instancias futuras de OpenStack que se creen a partir de este tipo.

Configurar la asignación de recursos de QoS para instancias mediante metadatos de imagen

Puede controlar las asignaciones de recursos de QoS, como límites, reservas y recursos compartidos, para CPU, RAM, IOPS de disco e interfaz de red virtual (VIF) al modificar los metadatos de la imagen de origen utilizada para crear la instancia. Todas las instancias creadas posteriormente a partir de la imagen heredan la configuración de metadatos.

La asignación de recursos de QoS para una instancia también puede especificarse a través de metadatos de tipo. Si se produce un conflicto, la configuración de metadatos de imagen anula la configuración de metadatos de tipo. Consulte Configurar la asignación de recursos de QoS para instancias mediante metadatos de tipo.

Requisitos previos

- Requiere VMware Integrated OpenStack versión 2.0.x o posterior.
- Requiere vSphere versión 6.0 o posterior.

- Compruebe que VMware Integrated OpenStack se esté ejecutando en vSphere.
- Compruebe si se encuentra conectado al panel de control de VMware Integrated OpenStack como administrador de nube.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione un proyecto de administración.

3 Seleccione **Administrador > Sistema > Imágenes**.

4 Haga clic en la imagen que desea modificar.

5 En la columna Acciones de la lista de imágenes, haga clic en la flecha hacia abajo y seleccione **Actualizar metadatos**.

6 En la columna debajo de Metadatos disponibles, expanda la pestaña **Cuota de VMware**.

Nota Si la pestaña **Cuota de VMware** no aparece, es posible que las propiedades de metadatos relacionadas ya estén configuradas.

7 Haga clic en el signo más (**+**) junto a la propiedad de metadatos de Cuota de VMware que desee agregar.

Sugerencia Para agregar todas las opciones a la vez, haga clic en el signo más (**+**) en la pestaña **Cuota de VMware**.

En la columna debajo de Metadatos existentes, aparecen las propiedades de metadatos recién agregadas.

8 Configure las propiedades de metadatos.

Propiedad de metadatos	Descripción
Cuota: límite de CPU	Aplica la propiedad de metadatos `quota_cpu_limit`. Especifica el límite superior para la asignación de CPU en MHz. Este parámetro garantiza que la instancia nunca use más que la cantidad definida de asignación de CPU. Escriba **`0`** para que la asignación de CPU sea ilimitada.
Cuota: reserva de CPU	Aplica la propiedad de metadatos `quota_cpu_reservation`. Especifica el mínimo de CPU de reserva garantizado en MHz. Este parámetro garantiza que la instancia tenga la cantidad reservada de ciclos de CPU disponible durante la contención de recursos.
Cuota: nivel de recursos compartidos de CPU	Aplica la propiedad de metadatos `quota_cpu_shares_level`. Especifica el nivel de recursos compartidos que se asigna al valor numérico predefinido de recursos compartidos. Si selecciona el nivel **`personalizado`**, debe incluir la propiedad de metadatos `quota_cpu_shares_value`. Vea Cuota: valor de recursos compartidos de CPU a continuación.

Propiedad de metadatos	Descripción
Cuota: valor de recursos compartidos de CPU	Aplica la propiedad de metadatos `quota_cpu_shares_value`. Especifica el número de recursos compartidos asignados a la instancia. Aplique esta propiedad solo si establece la propiedad de metadatos `quota_cpu_shares_level` como **`custom`**. De lo contrario, esta propiedad se ignorará.
Cuota: límite de E/S de disco	Aplica la propiedad de metadatos `quota_disk_io_limit`. Especifica el límite superior en segundos para las transacciones de disco en operaciones de E/S por segundo (IOPS). Este parámetro garantiza que la instancia nunca use más que la cantidad de IOPS de disco definida y puede usarse para aplicar un límite al rendimiento del disco de la instancia. Escriba **`0`** para que la cantidad de IOPS sea ilimitada.
Cuota: reserva de E/S de disco	Aplica la propiedad de metadatos `quota_disk_io_reservation`. Especifica el mínimo garantizado en segundos para las transacciones de disco en operaciones de E/S por segundo (IOPS). Este parámetro garantiza que la instancia reciba la cantidad reservada de IOPS de disco durante la contención de recursos.
Cuota: nivel de recursos compartidos de E/S de disco	Aplica la propiedad de metadatos `quota_disk_io_shares_level`. Especifica el nivel de recursos compartidos que se asigna al valor numérico predefinido de recursos compartidos. Si selecciona el nivel **`custom`**, debe incluir la propiedad de metadatos `quota_disk_io_shares_share` (Cuota: valor de recursos compartidos de E/S de disco).
Cuota: valor de recursos compartidos de E/S de disco	Aplica la propiedad de metadatos `quota_disk_io_shares_share`. Especifica el número de recursos compartidos asignados a la instancia. Aplique esta propiedad solo si establece la propiedad de metadatos `quota_disk_io_shares_level` como **`custom`**. De lo contrario, esta propiedad se ignorará.
Cuota: límite de memoria	Aplica la propiedad de metadatos `quota_memory_limit`. Especifica el límite superior para la asignación de memoria en MB. Este parámetro garantiza que la instancia nunca use más que la cantidad definida de memoria. Escriba **`0`** para que la asignación de memoria sea ilimitada.
Cuota: reserva de memoria	Aplica la propiedad de metadatos `quota_memory_reservation`. Especifica el mínimo garantizado de reserva de memoria en MB. Este parámetro garantiza que la instancia reciba la cantidad reservada de memoria durante la contención de recursos.
Cuota: nivel de recursos compartidos de memoria	Aplica la propiedad de metadatos `quota_memory_shares_level`. Especifica el nivel de recursos compartidos que se asigna al valor numérico predefinido de recursos compartidos. Si selecciona el nivel **`custom`**, debe incluir la propiedad de metadatos `quota_memory_shares_share` (Cuota: valor de recursos compartidos de memoria).
Cuota: valor de recursos compartidos de memoria	Aplica la propiedad de metadatos `quota_memory_shares_share`. Especifica el número de recursos compartidos asignados a la instancia. Aplique esta propiedad solo si establece la propiedad de metadatos `quota_memory_shares_level` como **`custom`**. De lo contrario, esta propiedad se ignorará.

Propiedad de metadatos	Descripción
Cuota: límite de VIF	Aplica la propiedad de metadatos `quota_vif_limit`. Especifica el límite superior para el ancho de banda VIF en Mbps. Este parámetro garantiza que VIF nunca use más que la cantidad definida de ancho de banda. Escriba **0** para que la asignación de ancho de banda sea ilimitada.
Cuota: reserva de VIF	Aplica la propiedad de metadatos `quota_vif_reservation`. Especifica el mínimo garantizado de ancho de banda para VIF en Mbps. Este parámetro garantiza que el adaptador virtual de la instancia obtenga la cantidad reservada de ancho de banda durante la contención de recursos. Si la instancia usa menos que la cantidad reservada, el resto queda disponible para otros adaptadores virtuales.
Cuota: nivel de recursos compartidos de VIF	Aplica la propiedad de metadatos `quota_vif_shares_level`. Especifica el nivel de recursos compartidos que se asigna al valor numérico predefinido de recursos compartidos. Si selecciona el nivel **`custom`**, debe incluir la propiedad de metadatos `quota_vif_shares_share` (Cuota: valor de recursos compartidos de VIF).
Cuota: valor de recursos compartidos de VIF	Aplica la propiedad de metadatos `quota_vif_shares_share`. Si se usa 'custom', este será el número de recursos compartidos.

9 Haga clic en **Guardar**.

Ahora los metadatos de imagen están configurados para límites, reservas y recursos compartidos de CPU, IOPS, memoria y ancho de banda de red. Esta configuración se aplicará a todas las instancias futuras de OpenStack que se creen a partir de esta imagen.

Aplicar asignación de recursos de QoS a instancias existentes

Para aplicar la configuración de asignación de recursos de QoS a una instancia existente, cambie el tamaño de la instancia en el panel VMware Integrated OpenStack.

Requisitos previos

- Requiere un tipo de OpenStack con la configuración de asignación de recursos de QoS deseada. Consulte Configurar la asignación de recursos de QoS para instancias mediante metadatos de tipo.
- Requiere VMware Integrated OpenStack versión 2.0.x o posterior.
- Compruebe que VMware Integrated OpenStack se esté ejecutando en vSphere.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack.

2 Seleccione **Administrador > Sistema > Instancias**.

3 Haga clic en el hipervínculo del nombre de la instancia para acceder a la página Detalles de la instancia.

4 Haga clic en la flecha hacia abajo (junto al botón **Crear snapshot**) y elija **Cambiar el tamaño de la instancia**.

5 En la pestaña **Elegir tipo**, abra la lista desplegable **Nuevo tipo** y seleccione el tipo que tenga las asignaciones de recursos de QoS que desee.

6 Haga clic en **Cambiar el tamaño**.

   El proceso de cambio de tamaño puede demorar unos minutos.

Ahora la instancia está sujeta a la configuración de QoS según se define en los metadatos del tipo.

Usar la administración basada en directivas de almacenamiento con instancias de OpenStack

Puede utilizar directivas de almacenamiento de vSphere para controlar los almacenes de datos en los que se crean instancias de OpenStack.

Requisitos previos

Cree la directiva de almacenamiento que desee en vSphere.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

3 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

4 Quite la marca de comentario del parámetro `nova_pbm_enabled` y establezca su valor como **`true`**.

5 Quite la marca de comentario del parámetro `nova_pbm_default_policy` y establezca su valor como el nombre de la directiva de almacenamiento que se utilizará de forma predeterminada al crear una instancia con un tipo que no esté asociado a una directiva de almacenamiento.

6 Quite la marca de comentario del parámetro `nova_scheduler_default_filters` y agregue **`AggregateInstanceExtraSpecsFilter`** al final.

```
nova_scheduler_default_filters: RetryFilter, AvailabilityZoneFilter, RamFilter, ComputeFilter,
ComputeCapabilitiesFilter, ImagePropertiesFilter, ServerGroupAntiAffinityFilter,
ServerGroupAffinityFilter, PciPassthroughFilter, AggregateInstanceExtraSpecsFilter
```

7 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

   Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

8 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

9 En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.

10 Seleccione **Administrador > Proceso > Tipos**.

11 Cree un nuevo tipo o elija uno existente.

12 Haga clic en **Actualizar metadatos** a la derecha del tipo.

13 En el panel **Metadatos disponibles**, expanda **Directivas de VMware** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Directiva de almacenamiento**.

14 Introduzca el nombre de la directiva de almacenamiento que desee como el valor del parámetro `vmware:storage_policy` y haga clic en **Guardar**.

La directiva de almacenamiento de vSphere especificada se aplica a todas las instancias nuevas de OpenStack que se creen a partir del tipo. La directiva de almacenamiento predeterminada se aplica a todas las instancias nuevas que se crean a partir de un tipo no asociado a ninguna directiva de almacenamiento.

Configurar la asignación de CPU virtual

Si ejecuta aplicaciones susceptibles a la latencia en una máquina virtual, con la asignación de CPU virtual puede eliminar la latencia adicional que conlleva la virtualización.

Importante Esta función solo está disponible en VMware Integrated OpenStack Carrier Edition. Para obtener más información, consulte "Licencias de VMware Integrated OpenStack" en la *Guía de instalación y configuración de VMware Integrated OpenStack*.

La asignación de CPU virtual habilita la sensibilidad de latencia alta y garantiza que toda la memoria y un núcleo físico completo estén reservados para la CPU virtual de una instancia de OpenStack. La asignación de CPU virtual se configura en un tipo y, a continuación, se crean instancias con dicho tipo.

Procedimiento

1 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

2 En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.

3 Seleccione **Administrador > Proceso > Tipos**.

4 Cree un nuevo tipo o elija uno existente para utilizarlo en la asignación de CPU virtual.

5 Seleccione la opción **Actualizar metadatos** que aparece junto al tipo que desea utilizar.

6 En el panel **Metadatos disponibles**, expanda **Asignación de CPU** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Directiva de asignación de CPU**.

7 Establezca el valor de `hw:cpu_policy` como **`dedicated`** y haga clic en **Guardar**.

Pasos siguientes

Ahora puede habilitar la asignación de CPU virtual en una instancia configurándola con el tipo que modificó en este procedimiento.

Configurar instancias de OpenStack para NUMA

VMware Integrated OpenStack admite la colocación con reconocimiento de acceso no uniforme a memoria (Non-Uniform Memory Access, NUMA) de las instancias de OpenStack en el entorno de vSphere subyacente.

Importante Esta función solo está disponible en VMware Integrated OpenStack Carrier Edition. Para obtener más información, consulte "Licencias de VMware Integrated OpenStack" en la *Guía de instalación y configuración de VMware Integrated OpenStack*.

NUMA vincula nodos pequeños y rentables mediante una conexión de alto rendimiento para proporcionar baja latencia y alta productividad. Este rendimiento a menudo es necesario para las funciones de red virtual (Virtual Network Function, VNF) de los entornos de telecomunicaciones. Para obtener información sobre NUMA en vSphere, consulte "Usar instancias de NUMA con ESXi" en *Administrar recursos de vSphere*.

Para obtener información sobre la configuración actual de NUMA, ejecute el siguiente comando en los hosts ESXi:

```
vsish –e get /net/pNics/vmnic<id>/properties | grep 'Device NUMA Node'
```

Requisitos previos

- Asegúrese de que las vCPU, la memoria y las NIC físicas destinadas al tráfico de máquina virtual se coloquen en el mismo nodo.
- En vSphere, cree una directiva de formación de equipos que incluya todas las NIC físicas en el nodo de NUMA. Consulte "Directiva de formación de equipos y conmutación por error" en *Redes de vSphere*.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

   ```
   sudo su –
   source ~/cloudadmin.rc
   ```

3. Cree una red de Neutron en la que se encuentren todas las NIC físicas en un único nodo de NUMA.
4. Cree un tipo de OpenStack que incluya la propiedad `numa.nodeAffinity`.

   ```
   nova flavor-key flavor-id set vmware:extra_config='{"numa.nodeAffinity": "numa-node-id"}'
   ```

5 Inicie una instancia de OpenStack con el tipo y la red que creó en este procedimiento.

Configurar dispositivos de acceso directo en instancias de OpenStack

Puede crear instancias de OpenStack utilizando dispositivos de acceso directo DirectPath I/O y Single Root I/O Virtualization (SR-IOV).

Importante Esta función solo está disponible en VMware Integrated OpenStack Carrier Edition. Para obtener más información, consulte "Licencias de VMware Integrated OpenStack" en la *Guía de instalación y configuración de VMware Integrated OpenStack*.

El acceso directo asocia un dispositivo físico con una máquina virtual, lo que reduce la latencia causada por la virtualización. En la tabla siguiente se muestra cómo se implementa el acceso directo en VMware Integrated OpenStack.

Tabla 6-1. Componentes y funciones clave de acceso directo

Componente	Función
Proceso para Nova	■ Recopila la lista de dispositivos SR-IOV y actualiza la lista de especificaciones de los dispositivos PCI. ■ Integra el ID de objeto del host en las especificaciones de los dispositivos.
Administrador de PCI de Nova	■ Crea y mantiene un grupo de dispositivos con dirección, ID de proveedor, ID de producto e ID de host. ■ Asigna y desasigna dispositivos PCI a instancias basadas en solicitudes PCI.
Programador de Nova	■ Programa la colocación de instancias en hosts que coincidan con las solicitudes PCI.
vSphere	■ Administra hosts en un clúster de proceso dedicado con NIC y hosts habilitados para SR-IOV. **Nota** Las reglas de DRS no se aplican a los dispositivos habilitados para SR-IOV. Coloque los hosts SR-IOV en un clúster de proceso independiente.

Configurar el acceso directo para los dispositivos de redes

Puede configurar un puerto para permitir el acceso directo de DirectPath I/O o de SR-IOV y, a continuación, crear instancias de OpenStack que usen interfaces de hardware físico.

Importante Esta función solo está disponible en VMware Integrated OpenStack Carrier Edition. Para obtener más información, consulte "Licencias de VMware Integrated OpenStack" en la *Guía de instalación y configuración de VMware Integrated OpenStack*.

Este procedimiento utiliza OpenStack Neutron para habilitar el acceso directo de dispositivos de redes. Para los dispositivos que no sean de redes, consulte Configurar el acceso directo para los dispositivos que no sean de redes.

Requisitos previos

- Habilite SR-IOV o DirectPath I/O en vSphere:
  - Para habilitar SR-IOV, consulte "Habilitar SR-IOV en un adaptador físico de host" en *Redes de vSphere*.
  - Para habilitar DirectPath I/O, consulte "Habilitar acceso directo de un dispositivo de red en un host" en *Redes de vSphere*.
- Cree un clúster de proceso dedicado para los dispositivos de SR-IOV. Las reglas de DRS no se aplican a estos dispositivos.
- Para mantener la persistencia de la dirección MAC de un dispositivo físico, agregue su clúster como un nodo informático antes de habilitar el acceso directo en el dispositivo. Si ya se habilitó el acceso directo, puede deshabilitarlo, reiniciar el clúster y volver a habilitar el acceso directo.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Si utiliza una implementación de NSX-T Data Center, especifique un conmutador distribuido para cada clúster de proceso en el que se habilita SR-IOV.
   a. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

   b. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
   c. Quite la marca de comentario del parámetro `nova_dvs_moid`.
   d. Especifique el nombre DNS de cada controlador informático en la implementación y el identificador de objeto administrado (Managed Object Identifier, MOID) de la instancia de VDS asociada a él.

   Por ejemplo:

   ```
   nova_dvs_moid:
      compute01: dvs–35
      compute02: dvs–36
   ```

   Tenga en cuenta que hay tres espacios antes del nombre de cada controlador informático.
   e. Implemente la configuración actualizada.

   ```
   sudo viocli deployment configure
   ```

   Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

3 Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su –
source ~/cloudadmin.rc
```

4 Cree una red de proveedor para los dispositivos de SR-IOV.

- Para las implementaciones de NSX Data Center for vSphere, cree una VLAN o una red de grupo de puertos.
- Para las implementaciones de NSX-T Data Center, cree una VLAN o una red opaca.

```
neutron net-create network-name --tenant-id project-uuid --provider:network_type {vlan | portgroup
| nsx-net} --provider:physical_network physical-id [--provider:segmentation_id vlan-id]
```

Opción	Descripción
network-name	Introduzca un nombre para la red.
--tenant-id	Especifique el UUID del proyecto para el que se va a crear el puerto. Puede encontrar el UUID de un proyecto ejecutando el comando `openstack project list`.
--provider:network_type	Introduzca **`vlan`** para una red VLAN, **`portgroup`** para una red de grupo de puertos o **`nsx-net`** para una red opaca.
--provider:physical_network	■ Para una red VLAN en NSX Data Center for vSphere, especifique el identificador de objeto administrado (Managed Object Identifier, MOID) del conmutador distribuido. ■ Para una red VLAN en NSX-T Data Center, especifique el UUID de la zona de transporte VLAN. ■ Para una red de grupo de puertos, especifique el MOID del grupo de puertos. ■ Para una red opaca, especifique el UUID del conmutador lógico.
--provider:segmentation_id	Si desea crear una red basada en VLAN, introduzca el identificador de VLAN.

5 Cree un puerto habilitado para acceso directo.

```
neutron port-create network-id --tenant-id project-uuid --name port-name --vnic_type {direct |
direct-physical}
```

Opción	Descripción
network-id	Especifique el UUID de la red en la que se va a crear el puerto. Puede encontrar el UUID de una red ejecutando el comando `openstack network list`.
--tenant-id	Especifique el UUID del proyecto para el que se va a crear el puerto.
--name	Introduzca un nombre para el puerto.
--vnic_type	Introduzca **`direct`** para SR-IOV o **`direct-physical`** para el acceso directo.

Nota La seguridad del puerto no es compatible con los puertos `direct` y `direct-physical`, y se deshabilitará automáticamente para el puerto que se creó.

Ahora puede implementar máquinas virtuales habilitadas para acceso directo configurándolas con el puerto que creó durante este procedimiento.

Configurar el acceso directo para los dispositivos que no sean de redes

Puede configurar los metadatos de imagen y tipo para permitir el acceso directo de DirectPath I/O o de SR-IOV y, a continuación, crear instancias de OpenStack que usen interfaces de hardware físico.

Importante Esta función solo está disponible en VMware Integrated OpenStack Carrier Edition. Para obtener más información, consulte "Licencias de VMware Integrated OpenStack" en la *Guía de instalación y configuración de VMware Integrated OpenStack*.

Este procedimiento utiliza OpenStack Nova para habilitar el acceso directo de dispositivos que no son de redes. Para los dispositivos de redes, consulte Configurar el acceso directo para los dispositivos de redes.

Requisitos previos

- Habilite SR-IOV o DirectPath I/O en vSphere:
  - Para habilitar SR-IOV, consulte "Habilitar SR-IOV en un adaptador físico de host" en *Redes de vSphere*.
  - Para habilitar DirectPath I/O, consulte "Habilitar acceso directo de un dispositivo de red en un host" en *Redes de vSphere*.
- Cree un clúster de proceso dedicado para los dispositivos de SR-IOV. Las reglas de DRS no se aplican a estos dispositivos.
- Para mantener la persistencia de la dirección MAC de un dispositivo físico, agregue su clúster como un nodo informático antes de habilitar el acceso directo en el dispositivo. Si ya se habilitó el acceso directo, puede deshabilitarlo, reiniciar el clúster y volver a habilitar el acceso directo.

Procedimiento

1. Inicie sesión en Servidor de administración de OpenStack como `viouser`.
2. Si la implementación no utiliza un archivo `custom.yml`, copie el archivo de plantilla `custom.yml` en el directorio `/opt/vmware/vio/custom`.

   ```
   sudo mkdir –p /opt/vmware/vio/custom
   sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
   ```

3. Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.
4. Quite la marca de comentario del parámetro `nova_pci_alias` y modifique su valor para que coincida con el dispositivo.

   ```
   nova_pci_alias: [{"device_type": "type–VF", "name": "virtual–device–name"}, {"vendor_id":"vid",
   "product_id":"pid", "device_type": "type–PF", "name":"physical–device–name"}]
   ```

El ejemplo anterior representa lo siguiente:

- `name` (primera aparición) es el alias del dispositivo virtual
- `vendor_id` es el identificador de cuatro dígitos del proveedor del dispositivo físico
- `device_id` es el identificador de cuatro dígitos del dispositivo físico
- `name` (segunda aparición) es el alias del dispositivo físico

5 Implemente la configuración actualizada.

```
sudo viocli deployment configure
```

Al implementar la configuración, se interrumpen brevemente los servicios de OpenStack.

6 Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.

7 En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.

8 Cree un tipo con el acceso directo habilitado.

a Seleccione **Administrador > Proceso > Tipos**.

b Cree un nuevo tipo o elija uno existente para utilizarlo para el acceso directo.

c Seleccione la opción **Actualizar metadatos** que aparece junto al tipo que desea utilizar.

d En el panel **Metadatos disponibles**, expanda **Opciones de controlador de VMware para tipos** y haga clic en el icono **Agregar** (signo más) que aparece junto al **alias de acceso directo de PCI**.

e Establezca el valor de `pci_passthrough:alias` en *`virtual-device-name`*`:`*`device-count`* y haga clic en **Guardar**.

Opción	Descripción
virtual-device-name	Introduzca el nombre del dispositivo virtual que especificó en el paso 4 de este procedimiento.
device-count	Especifique la cantidad de funciones virtuales que se pueden llamar en una solicitud. Este valor puede oscilar entre 1 y 10.

9 Cree una imagen con acceso directo habilitado.

a Seleccione **Administrador > Proceso > Imágenes**.

b Cree una nueva imagen o elija una existente para utilizarla para el acceso directo.

c Haga clic en la flecha abajo que aparece junto a la imagen que desea utilizar y seleccione **Actualizar metadatos**.

d En el panel **Metadatos disponibles**, expanda **Opciones de controlador de VMware** y haga clic en el icono **Agregar** (signo más) que aparece junto a la **interfaz de red virtual**.

e Seleccione el dispositivo de la lista desplegable que aparece junto al parámetro `hw_vif_model` y haga clic en **Guardar**.

Ahora puede implementar máquinas virtuales habilitadas para acceso directo configurándolas con el tipo y la imagen que modificó durante este procedimiento.

Solicitar un dispositivo compartido GPU para una instancia de OpenStack

Puede solicitar un dispositivo GPU compartido para una instancia de OpenStack al agregar un perfil de GPU a su implementación de VMware Integrated OpenStack y configurar una especificación adicional de tipo para solicitar el GPU virtual.

Requisitos previos

Compruebe que esté instalado el controlador adecuado para el dispositivo GPU en el host ESXi.

Procedimiento

1 Mediante SSH, inicie sesión en el servidor de administración de VMware Integrated OpenStack.

2 Si no existe, cree el archivo `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
     sudo cp /var/lib/vio/ansible/custom/custom.yml.sample
     /opt/vmware/vio/custom/custom.yml
```

3 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

4 Edite el archivo `custom.yml` para especificar el tamaño del búfer de cuadros y el perfil de GPU.

   a Edite el valor de `nova_gpu_profile` para especificar el perfil de GPU para todos los nodos informáticos; por ejemplo:

   ```
   nova_gpu_profile: grid_p100–4a
   ```

   b Edite el valor de `nova_profile_fb_size_kb` para especificar el tamaño del búfer de cuadros de GPU; por ejemplo:

   ```
   nova_profile_fb_size_kb: 4096
   ```

   c Guarde el archivo `custom.yml`.

5 Inserte la nueva configuración a la implementación de VMware Integrated OpenStack.

   La actualización de la configuración interrumpe brevemente los servicios de OpenStack.

   ```
   viocli deployment configure ––tags nova_api_config
   ```

6 Cree una especificación adicional de tipo para solicitar un GPU virtual.

   ```
   openstack flavor set vgpu_1 ––property "vmware:vgpu=1"
   ```

   VMware Integrated OpenStack es compatible con un GPU por máquina virtual.

7 Cree una instancia de OpenStack con el dispositivo GPU virtual.

```
openstack server create --flavor vgpu_1 --image cirros-0.3.5-x86_64-uec --wait test-vgpu
```

Tipos de OpenStack

7

En OpenStack, un tipo es una configuración preestablecida en la que se define la capacidad de proceso, memoria y almacenamiento de una instancia. Cuando se crea una instancia, se selecciona un tipo para configurar el servidor. Los usuarios administrativos pueden crear, editar y eliminar tipos.

No elimine ninguno de los tipos predeterminados.

Este capítulo incluye los siguientes temas:

Configuraciones de tipos predeterminados

La implementación predeterminada de OpenStack ofrece cinco tipos predeterminados, desde muy pequeño hasta extragrande.

Nombre	vCPU	RAM (MB)	Disco (GB)
m1.tiny	1	512	1
m1.small	1	2048	20
m1.medium	2	4096	40
m1.large	4	8192	80
m1.xlarge	8	16384	160

Crear un tipo

Los usuarios administrativos pueden crear tipos personalizados.

Requisitos previos

Compruebe si se encuentra conectado al panel de control de VMware Integrated OpenStack como administrador de nube.

Procedimiento

1. En el panel de control de VMware Integrated OpenStack, seleccione un proyecto de administración en el menú desplegable de la barra de título.
2. Seleccione **Administrador > Panel de sistema > Tipos**.
3. Haga clic en **Crear tipo**.
4. En el cuadro de diálogo Crear tipo, configure el nuevo tipo.

Parámetro	Descripción
Nombre	Nombre para el tipo.
ID	Valor entero o UUID4 para identificar al tipo. Si este parámetro queda vacío o contiene el valor **`auto`**, OpenStack genera un UUID automáticamente.
VCPUs	Cantidad de CPU virtuales que se utilizarán en una instancia creada a partir de este tipo.
RAM MB	Megabytes de memoria RAM para las máquinas virtuales creadas a partir de este tipo.
Gigabytes de disco raíz	Gigabytes de disco utilizados para la partición raíz (/) en las instancias creadas a partir de este tipo.
Gigabytes de disco efímero	Gigabytes de espacio en disco que se utilizarán para la partición efímera. Si no se especifica, el valor predeterminado es 0. Los discos efímeros ofrecen un almacenamiento en disco local para máquinas que se vincula con el ciclo de vida de una instancia de máquina virtual. Cuando se cierra la máquina virtual, se pierden todos los datos en el disco efímero. Los discos efímeros no se incluyen en las instantáneas.
Megabytes de disco de intercambio	Megabytes de espacio de intercambio para usar. Si no se especifica, el valor predeterminado es 0.

5. Haga clic en **Crear tipo** en la parte inferior del cuadro de diálogo para completar el proceso.
6. (opcional) Especifique los proyectos desde los que se podrá acceder a las instancias creadas a partir de tipos específicos.
   a. En la página Tipos, haga clic en la opción **Editar tipo** de la columna Acciones de la instancia.
   b. En el cuadro de diálogo Editar tipo, haga clic en la pestaña **Acceso al tipo**.
   c. Con los controles para alternar, seleccione los proyectos desde los que se podrá acceder a la instancia.
   d. Haga clic en **Guardar**.
7. (opcional) Modifique la configuración de un tipo específico.
   a. En la página Tipos, haga clic en la opción **Editar tipo** de la columna Acciones de la instancia.
   b. En el cuadro de diálogo Editar tipo, modifique las opciones de configuración de la pestaña **Info de tipo** o **Acceso al tipo**.
   c. Haga clic en **Guardar**.

Eliminar un tipo

Para administrar la cantidad y la variedad de tipos, se pueden eliminar los que ya no satisfacen las necesidades de los usuarios, los que duplican otros tipos o los que ya no son útiles por otros motivos.

Nota La eliminación de un tipo no se puede deshacer. No elimine los tipos predeterminados.

Requisitos previos

Se debe iniciar sesión en el panel de control de VMware Integrated OpenStack como administrador de la nube para realizar esta tarea.

Procedimiento

1. En el panel de control de VMware Integrated OpenStack, seleccione un proyecto de administración en el menú desplegable de la barra de título.
2. Seleccione **Administrador > Panel de sistema > Tipos**.
3. Seleccione los tipos que desea eliminar.
4. Haga clic en **Eliminar tipos**.
5. Cuando se le pregunte, confirme la eliminación.

Modificar metadatos de tipo

Puede modificar los metadatos de un tipo para agregar propiedades de forma dinámica a todas las instancias que usen dicho tipo que se creen en el futuro.

También puede usar metadatos de imagen para especificar varias configuraciones de metadatos de tipo. Si se produce un conflicto, la configuración de metadatos de imagen tendrá prioridad sobre la configuración de metadatos de tipo.

Requisitos previos

- Requiere VMware Integrated OpenStack versión 2.0.x o posterior.
- Requiere vSphere versión 6.0 o posterior.
- Compruebe que VMware Integrated OpenStack se esté ejecutando en vSphere.
- Compruebe si se encuentra conectado al panel de control de VMware Integrated OpenStack como administrador de nube.

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.
2. En el menú desplegable de la barra de título, seleccione un proyecto de administración.
3. Seleccione **Administrador > Sistema > Tipos**.

4 (opcional) Cree un tipo específico para el uso de la aplicación de metadatos.

   Cree un tipo personalizado que contenga la configuración específica. El tipo personalizado mantiene la configuración del tipo original intacta y disponible para la creación de otras instancias.

5 Seleccione el tipo que desea modificar.

6 En la columna Acciones de la lista de imágenes, haga clic en la flecha hacia abajo y seleccione **Actualizar metadatos**.

7 Haga clic en el signo más (**+**) junto a las propiedades de metadatos que desee agregar.

   En la columna debajo de Metadatos existentes, aparecen las propiedades de metadatos recién agregadas.

8 Configure las propiedades de metadatos.

   Por ejemplo, puede que deba seleccionar una opción de una lista desplegable o introducir un valor de cadena.

9 Haga clic en **Guardar**.

Se han configurado las propiedades de metadatos de tipo recién agregadas. Esta configuración se aplicará a todas las instancias futuras de OpenStack que se creen a partir de este tipo.

Especificaciones adicionales de tipos compatibles

Las especificaciones adicionales de tipos se utilizan para la configuración avanzada de instancias de proceso. VMware Integrated OpenStack expone capacidades adicionales a través de especificaciones adicionales de tipos.

Tabla 7-1. Especificaciones adicionales de tipos en VMware Integrated OpenStack

Especificación adicional	Descripción	Configurable mediante metadatos de imagen
`vmware:hw_version`	Especifique la versión de hardware que se utiliza para crear imágenes. En un entorno con versiones de host diferentes, puede usar esta clave para colocar instancias en los hosts correctos.	No
`vmware:latency_sensitivity_level`	Especifique el nivel de sensibilidad de latencia para las máquinas virtuales. Si se configura esta clave, se ajustará una configuración determinada en las máquinas virtuales.	SÍ

Tabla 7-1. Especificaciones adicionales de tipos en VMware Integrated OpenStack (Continuación)

Especificación adicional	Descripción	Configurable mediante metadatos de imagen
`vmware:storage_policy`	Especifique la directiva de almacenamiento usada para las nuevas instancias. Si no se habilita la administración basada en directivas de almacenamiento (Storage Policy-Based Management, SPBM), se omite este parámetro.	SÍ
`vmware:tenant_vdc`	Especifique el UUID del centro de datos virtual del tenant en el que se colocarán las instancias.	SÍ
`vmware:vm_group`	Especifique el grupo de máquinas virtuales de DRS en el que se colocarán las máquinas virtuales. Si el grupo de máquinas virtuales especificado no existe, las instancias no podrán encenderse.	SÍ
`hw:vifs_multi_thread`	Especifique **`true`** para proporcionar a cada interfaz virtual su propio subproceso de transmisión.	No
`quota:cpu_limit`	Especifique la asignación máxima de CPU en MHz. El valor `0` indica que el uso de CPU no es limitado.	SÍ
`quota:cpu_reservation`	Especifica la asignación garantizada de CPU en MHz.	SÍ
`quota:cpu_reservation_percent`	Especifica la asignación garantizada de CPU como un porcentaje de la velocidad de CPU real de la instancia. Este parámetro tiene prioridad sobre el parámetro `cpu_reservation`.	SÍ
`quota:cpu_shares_level`	Especifica el nivel de recursos compartidos de CPU asignados. Puede introducir **`custom`** y agregar el parámetro `cpu_shares_share` para proporcionar un valor personalizado.	SÍ
`quota:cpu_shares_share`	Especifica el número de recursos compartidos de CPU asignados. Si no se establece el parámetro `cpu_shares_level` como `custom`, se omite este valor.	SÍ

Tabla 7-1. Especificaciones adicionales de tipos en VMware Integrated OpenStack (Continuación)

Especificación adicional	Descripción	Configurable mediante metadatos de imagen
`quota:memory_limit`	Especifique la asignación de memoria máxima en MB. El valor `0` indica que el uso de memoria no es limitado.	SÍ
`quota:memory_reservation`	Especifique la asignación de memoria garantizada en MB.	SÍ
`quota:memory_reservation_percent`	Especifique la asignación de memoria garantizada como un porcentaje de la memoria real de la instancia. El valor `100` indica que la memoria invitada también está completamente reservada. Este parámetro tiene prioridad sobre el parámetro `memory_reservation`.	SÍ
`quota:memory_shares_level`	Especifica el nivel de recursos compartidos de memoria asignados. Puede introducir **`custom`** y agregar el parámetro `memory_shares_share` para proporcionar un valor personalizado.	SÍ
`quota:memory_shares_share`	Especifica el número de recursos compartidos de memoria asignados. Si no se establece el parámetro `memory_shares_level` como `custom`, se omite este valor.	SÍ
`quota:disk_io_limit`	Especifique la asignación de transacciones de disco máxima en E/S por segundo. El valor `0` indica que las transacciones de disco no son limitadas.	SÍ
`quota:disk_io_reservation`	Especifique la asignación de transacciones de disco garantizadas en E/S por segundo.	SÍ
`quota:disk_io_shares_level`	Especifica el nivel de recursos compartidos de transacciones de disco asignados. Puede introducir **`custom`** y agregar el parámetro `disk_io_shares_share` para proporcionar un valor personalizado.	SÍ

Tabla 7-1. Especificaciones adicionales de tipos en VMware Integrated OpenStack (Continuación)

Especificación adicional	Descripción	Configurable mediante metadatos de imagen
`quota:disk_io_shares_share`	Especifica el número de recursos compartidos de transacciones de disco asignados. Si no se establece el parámetro `disk_io_shares_level` como `custom`, se omite este valor.	SÍ
`quota:vif_limit`	Especifique la asignación máxima de ancho de banda de la interfaz virtual en Mbps. El valor `0` indica que el ancho de banda de la interfaz virtual no es limitado.	SÍ
`quota:vif_reservation`	Especifique la asignación garantizada de ancho de banda de la interfaz virtual en Mbps.	SÍ
`quota:vif_shares_level`	Especifica el nivel de recursos compartidos de ancho de banda de la interfaz virtual asignados. Puede introducir **`custom`** y agregar el parámetro `vif_shares_share` para proporcionar un valor personalizado.	SÍ
`quota:vif_shares_share`	Especifica el número de recursos compartidos de ancho de banda de la interfaz virtual asignados. Si no se establece el parámetro `disk_io_shares_level` como `custom`, se omite este valor.	SÍ

Volúmenes y tipos de volumen de Cinder 8

Los volúmenes son dispositivos de almacenamiento en bloque que se conectan a las instancias para habilitar el almacenamiento persistente.

Como administrador de nube, puede administrar volúmenes y tipos de volumen para usuarios en distintos proyectos. Puede crear y eliminar tipos de volúmenes, y también puede ver y eliminar volúmenes.

Los usuarios de la nube pueden asociar un volumen a una instancia en ejecución, o bien desasociar un volumen y asociarlo a otra instancia en cualquier momento. Para obtener información acerca de las operaciones de usuario de nube, consulte "Trabajar con volúmenes" en la *Guía de usuario de VMware Integrated OpenStack*.

Este capítulo incluye los siguientes temas:

Crear un tipo de volumen

Puede crear tipos de volumen y exponerlos a uno o varios tenants para su uso en la creación de volúmenes. Los tipos de volumen pueden definir la configuración del cifrado de volumen, el perfil de almacenamiento de vSphere correspondiente y el tipo de adaptador predeterminado.

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.
2. En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.
3. Seleccione **Administrador > Volumen > Tipos de volumen** y haga clic en **Crear tipo de volumen**.
4. Introduzca un nombre y una descripción para el tipo de volumen.

5 Si desea que el tipo de volumen esté disponible solo para determinados proyectos, anule la selección de la opción **Público**.

Puede configurar el acceso al tipo de volumen después de crearlo.

6 Haga clic en **Crear tipo de volumen**.

El nuevo tipo de volumen se muestra en la lista **Tipos de volumen**.

7 Si desea configurar el cifrado para el tipo de volumen, siga estos pasos:

Nota No se puede agregar ni actualizar el cifrado cuando un volumen utiliza el tipo de volumen.

a En la columna **Acciones**, seleccione **Crear cifrado**.

b Configure el cifrado como se indica a continuación.

Opción	Descripción
Proveedor	Introduzca la clase que proporciona el cifrado.
Ubicación de control	Seleccione **front-end** o **back-end**.
Clave de cifrado	(Opcional) Introduzca el algoritmo de cifrado. Si no introduce ningún valor, se utilizará el valor predeterminado del proveedor especificado.
Tamaño de clave (bits)	(Opcional) Introduzca el tamaño de la clave de cifrado en bits. Si no introduce ningún valor, se utilizará el valor predeterminado del proveedor especificado.

c Haga clic en **Crear cifrado de tipo de volumen**.

8 Si desea asociar un perfil de almacenamiento de vSphere con el tipo de volumen, siga estos pasos:

a En la columna **Acciones**, seleccione **Ver especificaciones adicionales**.

b Haga clic en **Crear**.

c Escriba **`vmware:storage_profile`** en el cuadro de texto **Clave**.

d Introduzca el nombre del perfil de almacenamiento de vSphere en el cuadro de texto **Valor**.

e Haga clic en **Crear**.

9 Si desea establecer un adaptador predeterminado para el tipo de volumen, siga estos pasos:

a En la columna **Acciones**, seleccione **Ver especificaciones adicionales**.

b Haga clic en **Crear**.

c Escriba **`vmware:adapter_type`** en el cuadro de texto **Clave**.

d Introduzca el tipo de adaptador en el cuadro de texto **Valor**.

Se admiten los siguientes valores: **`lsiLogic`**, **`busLogic`**, **`lsiLogicsas`**, **`paraVirtual`** e **`ide`**.

e Haga clic en **Crear**.

10 Si el tipo de volumen no es público, seleccione **Editar acceso** en la columna **Acciones** y especifique los proyectos que podrán utilizar el tipo de volumen.

   Si no especifica ningún proyecto, solo los administradores de nube podrán ver el tipo de volumen.

Los tenants pueden seleccionar un tipo de volumen al crear un volumen o al modificar uno existente. A continuación, la configuración definida por el tipo de volumen especificado se aplicará al nuevo volumen.

Pasos siguientes

Si desea cambiar el nombre o la descripción de un tipo de volumen, haga clic en **Editar tipo de volumen** en la columna **Acciones** y realice los cambios que desee. Para eliminar tipos de volumen que no sean necesarios, selecciónelos de la tabla **Tipos de volumen** y haga clic en **Eliminar tipos de volumen**.

Modificar el tipo de adaptador predeterminado de un volumen de Cinder

A partir de VMware Integrated OpenStack 3.1, es posible cambiar el tipo de adaptador predeterminado por los volúmenes recientemente creados. Para ello, se debe cambiar el parámetro `vmware_adapter_type` mediante un archivo `custom.yml`.

De manera predeterminada, los volúmenes vacíos siempre se crean y asocian a un controlador de lsiLogic. Cuando un volumen se crea a partir de una imagen, Cinder respeta la propiedad `vmware_adaptertype` de la imagen y crea el controlador correspondiente. Para los volúmenes recientemente creados, el tipo de adaptador se establece con el parámetro `cinder_volume_default_adapter_type` en el archivo `custom.yml` con uno de los siguientes valores.

Valor	Descripción
lsiLogic	Establece el tipo de adaptador predeterminado en LSI Logic.
busLogic	Establece el tipo de adaptador predeterminado en Bus Logic.
lsiLogicsas	Establece el tipo de adaptador predeterminado en LSI Logic SAS.
paraVirtual	Establece el tipo de adaptador predeterminado en VMware Paravirtual SCSI.
ide	Establece el tipo de adaptador predeterminado en IDE.

Procedimiento

1 Implemente el archivo `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

   a Quite la marca de comentario del parámetro `cinder_volume_default_adapter_type`.

   b Cambie la configuración con un valor personalizado, por ejemplo, **`lsiLogicsas`**.

```
############################
# cinder-volume options
############################

# Default volume adapter type; valid values are 'lsiLogic',
# 'busLogic', 'lsiLogicsas', 'paraVirtual' and 'ide'. (string value)
#cinder_volume_default_adapter_type: 'lsiLogicsas'
```

3 Guarde el archivo `custom.yml`.

4 Inserte la nueva configuración a la implementación de VMware Integrated OpenStack.

```
viocli deployment configure
```

Nota Al insertar la configuración, se interrumpen brevemente los servicios de OpenStack.

Configurar el formato de la instantánea de volumen

La plantilla de vSphere es el formato predeterminado de la instantánea de volumen para un vCenter Server. Esto permite que VMware Integrated OpenStack tome instantáneas de volúmenes asociados a instancias.

Para cambiar el formato de la instantánea al formato de disco de copia en escritura utilizado en VMware Integrated OpenStack 4.1 o anterior, establezca el parámetro de `cinder_vmware_snapshot_format` mediante un archivo `custom.yml`.

Procedimiento

1 Implemente el archivo `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

   a Quite la marca de comentario del parámetro `cinder_vmware_snapshot_format`.

   b Establezca el valor en **`COW`**.

```
cinder_vmware_snapshot_format: COW
```

3 Guarde el archivo `custom.yml`.

4 Inserte la nueva configuración a la implementación de VMware Integrated OpenStack.

```
viocli deployment configure
```

Nota Al insertar la configuración, se interrumpen brevemente los servicios de OpenStack.

Migración de volúmenes entre almacenes de datos

Puede migrar volúmenes Cinder entre almacenes de datos de forma segura. Esta migración le permite reemplazar almacenes de datos, aumentar la cantidad de recursos y la capacidad, y preservar los volúmenes sin tener que dejarlos sin conexión. El proceso de migración de volúmenes depende de diversos factores. Por ejemplo, el proceso es muy simple si el volumen no está asociado a una instancia. Si lo está, deberá migrar la instancia.

Nota No se puede migrar ningún volumen que tenga snapshots asociadas. Primero debe desasociarlas.

Migrar todos los volúmenes de un almacén de datos especificado

Es posible evacuar de forma rápida todos los volúmenes de un almacén de datos especificado y migrarlos automáticamente a otros almacenes de datos del mismo clúster de almacén de datos.

Requisitos previos

- Compruebe que el almacén de datos especificado forme parte de un clúster de almacén de datos.
- Compruebe que Storage DRS se encuentre habilitado en `Not Automation (Manual Mode)` para el clúster de almacén de datos.
- Compruebe que el volumen no contenga ninguna snapshot asociada. Si contiene una, primero es necesario desasociarla.

Procedimiento

1 Mediante SSH, inicie sesión en VMware Integrated OpenStack Manager.

2 Pase a usar el usuario raíz.

```
sudo su –
```

3 Prepare el volumen para la migración.

Este paso prepara todos los volúmenes del almacén de datos especificado para la migración.

```
viocli ds-migrate-prep [-d DEPLOYMENT] DC_NAME DS_NAME
```

Opción	Descripción
-d DEPLOYMENT	Indica el nombre de la implementación de VMware Integrated OpenStack.
DC_NAME	Indica el nombre del centro de datos.
DS_NAME	Indica el nombre del almacén de datos.

4 Coloque el almacén de datos en modo de mantenimiento.

Consulte la documentación del producto vSphere.

Cuando el almacén de datos se coloca en modo de mantenimiento, se evacúa el almacén de datos y los volúmenes se migran automáticamente a otros almacenes de datos del mismo clúster de almacén de datos.

Migrar volúmenes Cinder no asociados

Es posible migrar a almacenes de datos de destino especificados los volúmenes Cinder que no se asociaron a ninguna instancia.

Requisitos previos

Compruebe que el volumen no contenga ninguna snapshot asociada. Si contiene una, primero es necesario desasociarla.

Procedimiento

1 Mediante SSH, inicie sesión en VMware Integrated OpenStack Manager.

2 Pase a usar el usuario raíz.

```
sudo su -
```

3 Migre el volumen.

```
viocli volume-migrate [-d NAME] {--volume-ids UUID1[,UUID2...] | --source-dc SRC-DC-NAME --source-ds SRC-DS-NAME] DEST-DC-NAME DEST-DS-NAME [--ignore-storage-policy]
```

Para obtener más información sobre este comando, consulte la documentación de Comando viocli volume-migrate.

Migrar volúmenes Cinder asociados

Para migrar un volumen de Cinder asociado a un almacén de datos diferente, es necesario migrar la máquina virtual correspondiente a la instancia a la que se asocia.

Requisitos previos

Desasocie las instantáneas que están asociadas al volumen.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack y prepare el volumen para la migración.

Este paso prepara todos los volúmenes del almacén de datos especificado para la migración.

```
sudo viocli ds-migrate-prep dc-name ds-name
```

Opción	Descripción
DC_NAME	Introduzca el centro de datos que contiene el volumen deseado.
DS_NAME	Introduzca el almacén de datos que contiene el volumen deseado.

2 En vSphere Client, busque la máquina virtual correspondiente a la instancia de proceso a la que está asociado el volumen.

3 Utilice Storage vMotion para migrar la máquina virtual a un almacén de datos diferente.

El volumen se migra al nuevo almacén de datos, pero solo el disco de la máquina virtual de sombra se transfiere al nuevo almacén de datos. La máquina virtual de sombra permanece en el almacén de datos anterior sin disco.

4 (opcional) Para reparar el disco de la máquina virtual de sombra, ejecute un procedimiento para desasociar el volumen.

La operación de desasociación desconectará el volumen de la instancia. Es posible que se produzcan errores de lectura o escritura del volumen.

Especificaciones adicionales de tipos de volúmenes compatibles

Las especificaciones adicionales de tipos de volúmenes se utilizan para la configuración avanzada de volúmenes de Cinder. VMware Integrated OpenStack expone capacidades adicionales a través de especificaciones adicionales de tipos de volúmenes.

Tabla 8-1. Especificaciones adicionales de tipos de volúmenes en VMware Integrated OpenStack

Especificación adicional	Descripción
`vmware:vmdk_type`	Especifique el formato de aprovisionamiento de volúmenes de Cinder en vSphere. Puede especificar los siguientes formatos: ■ Aprovisionamiento fino: `thin` ■ Puesta a cero lenta con aprovisionamiento grueso: `thick` ■ Puesta a cero rápida con aprovisionamiento grueso: `eagerZeroedThick`
`vmware:clone_type`	Especifique el tipo de clonación. Puede especificar los siguientes tipos: ■ Clon completo: `full` ■ Clon vinculado: `linked`
`vmware:storage_profile`	Introduzca el nombre de la directiva de almacenamiento que se utilizará para los volúmenes nuevos.
`vmware:adapter_type`	Especifique el tipo de adaptador que se utiliza para asociar el volumen. Puede especificar los siguientes tipos: ■ IDE: `ide` ■ LSI Logic: `lsiLogic` ■ LSI Logic SAS: `lsiLogicsas` ■ BusLogic paralelo: `busLogic` ■ VMware Paravirtual SCSI: `paraVirtual`

Imágenes de Glance

9

En el contexto de OpenStack, una imagen es un archivo con un disco virtual a partir del cual se puede instalar un sistema operativo en una máquina virtual. Para crear una instancia en la nube de OpenStack, se debe utilizar una de las imágenes disponibles.

El componente del servicio de imágenes de VMware Integrated OpenStack admite de forma nativa imágenes empaquetadas en los formatos ISO, OVA y VMDK. También puede importar imágenes RAW, QCOW2, VDI y VHD, las cuales se convierten automáticamente al formato VMDK durante el proceso de creación de imágenes.

Este capítulo incluye los siguientes temas:

Importar imágenes mediante la GUI

Puede importar imágenes en el panel de control de VMware Integrated OpenStack.

Se admiten los siguientes formatos de imagen:

- VMDK
- ISO
- OVA
- RAW
- QCOW2
- VDI

- VHD

Nota Las imágenes ISO no puede usarse para crear volúmenes.

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube.
2. En el menú desplegable de la barra de título, seleccione el proyecto de **admin**.
3. Seleccione **Administrador > Proceso > Imágenes** y haga clic en **Crear imagen**.
4. Configure la imagen.

Opción	Acción
Nombre de imagen	Introduzca un nombre para la imagen.
Descripción de imagen	Introduzca una descripción para la imagen.
Origen de imagen	Seleccione el archivo de imagen.
Formato	Seleccione **ISO** o **VMDK**. Para las imágenes con formato OVA, RAW, QCOW2, VDI o VHD, seleccione **VMDK** como formato de disco.
Tipo de adaptador de disco	Para las imágenes VMDK, seleccione el tipo de adaptador.
Disco mínimo (GB)	Especifique el tamaño de disco mínimo para la imagen en gigabytes.
RAM mínima (MB)	Especifique la memoria RAM mínima para la imagen en megabytes.
Visibilidad	Seleccione **Pública** para que la imagen esté disponible para todos los proyectos o **Privada** para que esté disponible únicamente para el proyecto actual.
Protegida	Seleccione **Sí** para evitar que se elimine la imagen.

5. (opcional) Haga clic en **Siguiente** y configure los metadatos de la imagen.
6. Haga clic en **Crear imagen**.

Pasos siguientes

Los tenants pueden iniciar instancias de OpenStack mediante la imagen importada. Para obtener instrucciones, consulte "Iniciar una instancia de OpenStack a partir de una imagen" en la *Guía del usuario de VMware Integrated OpenStack*.

En la columna **Acciones** junto a una imagen, puede editar la imagen, actualizar sus metadatos, eliminar la imagen o crear un volumen a partir de la imagen.

Importar imágenes mediante la CLI

Puede importar imágenes mediante la interfaz de línea de comandos en Servidor de administración de OpenStack.

Se admiten los siguientes formatos de imagen:

- VMDK
- ISO

- OVA
- RAW
- QCOW2
- VDI
- VHD

Nota Las imágenes ISO no puede usarse para crear volúmenes.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Cambie al usuario `root` y cargue el archivo de credenciales del administrador de nube.

```
sudo su -
source ~/cloudadmin.rc
```

3 Cree la imagen en Glance.

```
openstack image create image-name --disk-format {vmdk | iso} --container-format bare --file image-file {--public | --private} [--property vmware_adaptertype="vmdk-adapter-type" [--property vmware_disktype="{sparse | preallocated | streamOptimized}"] --property vmware_ostype="operating-system"
```

Opción	Descripción
image-name	Introduzca el nombre de la imagen de origen.
--disk-format	Introduzca el formato de disco de la imagen de origen. Puede especificar `iso` o `vmdk`. Para las imágenes en otros formatos (incluidos OVA, RAW, QCOW2, VDI o VHD), utilice `vmdk` como formato de disco.
--container-format	Introduzca **`bare`**. Actualmente, Glance no utiliza el argumento de formato de contenedor.
--file	Especifique el archivo de imagen que va a cargar.
{--public | --private}	Incluya `--public` para que la imagen esté disponible para todos los usuarios o `--private` para que la imagen esté disponible únicamente para el usuario actual.
--property vmware_adaptertype	Especifique el tipo de adaptador del disco VMDK. Si no incluye este parámetro, el tipo de adaptador se determina por introspección. **Nota** ■ Para los discos que usan adaptadores paravirtuales, incluya este parámetro y establézcalo como **`paraVirtual`**. ■ Para los discos que usan adaptadores LSI Logic SAS, incluya este parámetro y establézcalo como **`lsiLogicsas`**.

Opción	Descripción
--property vmware_disktype	Especifique **sparse**, **preallocated** o **streamOptimized**. Si no incluye este parámetro, el tipo de disco se determina por introspección.
--property vmware_ostype	Especifique el sistema operativo en la imagen.

Pasos siguientes

Puede ejecutar el comando `openstack image list` para ver el nombre y el estado de las imágenes en la implementación.

Los tenants pueden iniciar instancias de OpenStack mediante la imagen importada. Para obtener instrucciones, consulte "Iniciar una instancia de OpenStack a partir de una imagen" en la *Guía del usuario de VMware Integrated OpenStack*.

Agregar una plantilla de máquina virtual como imagen

Puede agregar plantillas de máquina virtual existentes a la implementación de VMware Integrated OpenStack como imágenes de Glance. Esto permite a los usuarios arrancar instancias, crear volúmenes de almacenamiento en bloque de arranque y usar otras funciones disponibles para las imágenes de Glance.

Requisitos previos

- Compruebe que la plantilla de máquinas virtuales existente resida en el mismo vCenter Server que la implementación de VMware Integrated OpenStack.
- Compruebe que se cumplan las siguientes condiciones.
  - La plantilla de máquina virtual no contiene varios discos.
  - La plantilla de máquina virtual no contiene una unidad de CD-ROM.
  - La plantilla de máquina virtual no contiene una unidad de disquete.

Procedimiento

1 Prepare la plantilla de máquina virtual.

  Configure las opciones de metadatos según sea necesario.

  - `vmware_ostype` es obligatorio para las imágenes de Windows, pero es opcional para las imágenes de Linux.
  - Se recomienda `hw_vif_model` para especificar el tipo de NIC. Antes de definir esta opción de configuración, confirme que el tipo de NIC sea correcto para esta plantilla de imagen. Por ejemplo, si esta opción queda sin definir, la instancia se aprovisiona con la NIC E1000 de forma predeterminada. Para asegurarse de que se aprovisione con otra NIC, defina esta opción de configuración según corresponda.

    Por ejemplo, para aprovisionar la NIC VMXNET3, la definición de metadatos debe ser **`hw_vif_model=VirtualVmxnet3`**.

- Los siguientes ajustes de los metadatos no son obligatorios.
  - `vmware_adaptertype`
  - `vmware_disktype`

2 Inicie sesión en el clúster de administración de OpenStack.

3 Ejecute el comando `glance` para obtener, definir e importar la imagen.

```
glance image-create --name <NAME> \
       --disk-format vmdk --container-format bare
       --property vmware_ostype=ubuntu64Guest
       --property hw_vif_model=VirtualVmxnet3

glance location-add <glance_image_UUID> --url "vi://<vcenter-host>/<datacenter-path>/vm/<sub-
folders>/<template_name> IMAGE_ID"
```

El comando `location-add` señala la ruta de acceso al inventario de la plantilla de máquina virtual y puede hacer referencia a una máquina virtual o a un host. Por ejemplo:

```
"vi://<datacenter-path>/vm/<template_name>”
or
"vi://<datacenter-path>/host/<host_name>/<template_name>"
```

Las palabras clave `vm` y `host` en la ruta de acceso del inventario representan la jerarquía de **Vista de máquinas virtuales y plantillas** y **Vista de hosts y clústeres** en vSphere.

Migrar una imagen existente

Puede migrar imágenes entre almacenes de datos de modo que conserven el UUID y los metadatos.

Requisitos previos

Compruebe que tanto el almacén de datos actual como el de destino están disponibles.

Procedimiento

1 Inicie sesión en el nodo controller01 mediante SSH.

2 Pase a usar el usuario raíz.

```
sudo su –
```

3 Vea una lista de imágenes.

```
openstack image list
```

El resultado enumera los UUID, los nombres y los estados de las imágenes.

```
+--------------------------------------+-----------------------------------+--------+
| ID                                   | Name                              | Status |
+--------------------------------------+-----------------------------------+--------+
| 00acfc1f-2109-4e9c-b628-de7149b42dc3 | ubuntu-16.04-server-cloudimg-amd64 | Active |
| bf1abfb8-8bcc-4ce8-a9e8-3432b8ca546e | ubuntu1604_jenkins_node            | Active |
+--------------------------------------+-----------------------------------+--------+
```

4 Determine el UUID del proyecto.

```
openstack project list --domain default
```

El resultado muestra el UUID y el nombre del proyecto.

```
+----------------------------------+-------+
| ID                               | Name  |
+----------------------------------+-------+
| f33350f3844948fcb482ed6f5eef133d | admin |
+----------------------------------+-------+
```

5 Inicie sesión en vSphere Web Client.

6 Desplácese hasta vCenter y busque la carpeta del proyecto con el UUID del proyecto.

7 En la carpeta del proyecto, busque la plantilla con el UUID de la imagen.

8 Haga clic con el botón secundario en la plantilla y seleccione **Clonar en plantilla** para abrir el asistente Plantilla a plantilla:

a Escriba un nombre nuevo para la plantilla.

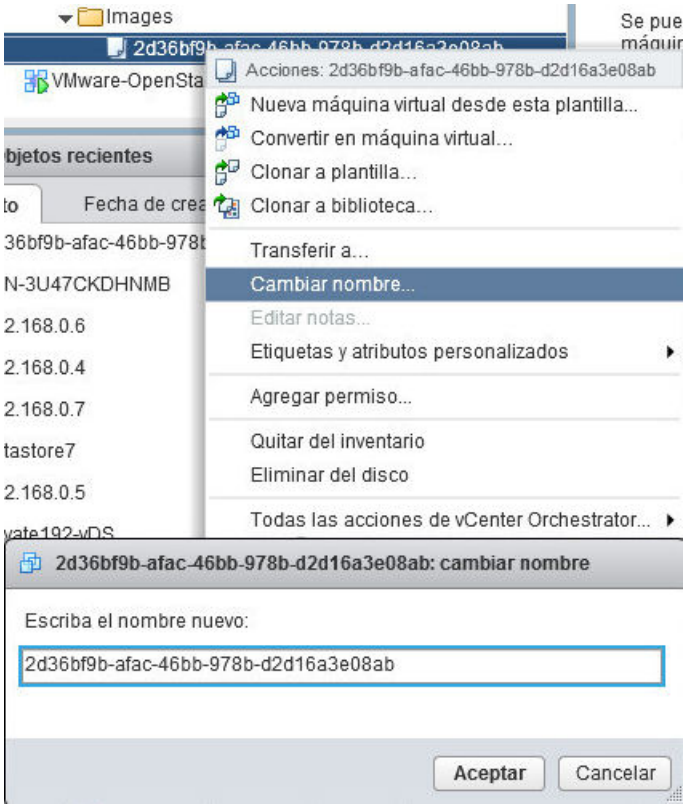
b Seleccione un host diferente.

c Elija un almacén de datos.

d Haga clic en **Finalizar** para completar la nueva plantilla.

9 Haga clic con el botón secundario en la plantilla original y seleccione **Eliminar del disco**.

10 Haga clic con el botón secundario en la plantilla clonada y seleccione **Cambiar nombre** para escribir el nombre original como el nuevo nombre.



Modificar el comportamiento predeterminado de los snapshots de Nova

De forma predeterminada, los snapshots de Nova son imágenes de Glance que se almacenan y organizan como plantillas de máquina virtual en el vCenter Server configurado para VMware Integrated OpenStack. Puede modificar este comportamiento de manera que, en su lugar, las instantáneas se almacenen como discos VMDK optimizados para transmisión.

Antes de VMware Integrated OpenStack 2.5, el comportamiento predeterminado consistía en almacenar instantáneas de Nova como discos VMDK optimizados para transmisión. Este procedimiento permite restaurar el valor predeterminado anterior a la versión 2.5.

Procedimiento

1 Implemente el archivo `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

   a Quite la marca de comentario del parámetro `nova_snapshot_format`.

   b Cambie la configuración a **`streamOptimized`**.

```
############################
# Glance Template Store
# options that affect the use of glance template store
############################
#glance_default_store: vi
nova_snapshot_format: streamOptimized
#cinder_image_format: template
```

3 Guarde el archivo `custom.yml`.

4 Inserte la nueva configuración a la implementación de VMware Integrated OpenStack.

```
viocli deployment configure
```

Nota Al insertar la configuración, se interrumpen brevemente los servicios de OpenStack.

Modificar el comportamiento upload-to-image predeterminado de Cinder

De forma predeterminada, la característica upload-to-image del almacenamiento en bloque crea una imagen de Glance a partir de un volumen de Cinder que se almacena y se organiza como una plantilla de máquina virtual. Puede modificar este comportamiento para que las imágenes se almacenen como discos VMDK streamOptimized.

Antes de VMware Integrated OpenStack 2.5, el comportamiento predeterminado consistía en almacenar las imágenes de Glance como discos VMDK streamOptimized. Este procedimiento permite restaurar el valor predeterminado anterior a la versión 2.5.

Procedimiento

1 Implemente el archivo `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
     sudo cp /var/lib/vio/ansible/custom/custom.yml.sample
     /opt/vmware/vio/custom/custom.yml
```

2 Abra el archivo `/opt/vmware/vio/custom/custom.yml` en un editor de texto.

   a Quite la marca de comentario del parámetro `cinder_image_format`.

   b Cambie la configuración a **`streamOptimized`**.

```
############################
# Glance Template Store
# options that affect the use of glance template store
############################
#glance_default_store: vi
#nova_snapshot_format: template
cinder_image_format: streamOptimized
```

3 Guarde el archivo `custom.yml`.

4 Inserte la nueva configuración a la implementación de VMware Integrated OpenStack.

```
viocli deployment configure
```

Nota Al insertar la configuración, se interrumpen brevemente los servicios de OpenStack.

Metadatos de imagen admitidos

Los metadatos de imagen se utilizan para la configuración avanzada de imágenes de Glance. VMware Integrated OpenStack expone capacidades adicionales por medio de los metadatos de imagen.

Tabla 9-1. Metadatos de imagen en VMware Integrated OpenStack

Especificación adicional	Descripción
`vmware_latency_sensitivity_level`	Especifique el nivel de sensibilidad de latencia para las máquinas virtuales. Si se configura esta clave, se ajustará una configuración determinada en las máquinas virtuales.
`vmware_storage_policy`	Especifique la directiva de almacenamiento usada para las nuevas instancias. Si no se habilita la administración basada en directivas de almacenamiento (Storage Policy-Based Management, SPBM), se omite este parámetro.
`vmware_tenant_vdc`	Especifique el UUID del centro de datos virtual del tenant en el que se colocarán las instancias.
`vmware_vm_group`	Especifique el grupo de máquinas virtuales de DRS en el que se colocarán las máquinas virtuales. Si el grupo de máquinas virtuales especificado no existe, las instancias no podrán encenderse.
`quota_cpu_limit`	Especifique la asignación máxima de CPU en MHz. El valor `0` indica que el uso de CPU no es limitado.
`quota_cpu_reservation`	Especifica la asignación garantizada de CPU en MHz.

Tabla 9-1. Metadatos de imagen en VMware Integrated OpenStack (Continuación)

Especificación adicional	Descripción
`quota_cpu_reservation_percent`	Especifica la asignación garantizada de CPU como un porcentaje de la velocidad de CPU real de la instancia. Este parámetro tiene prioridad sobre el parámetro `cpu_reservation`.
`quota_cpu_shares_level`	Especifica el nivel de recursos compartidos de CPU asignados. Puede introducir **`custom`** y agregar el parámetro `cpu_shares_share` para proporcionar un valor personalizado.
`quota_cpu_shares_share`	Especifica el número de recursos compartidos de CPU asignados. Si no se establece el parámetro `cpu_shares_level` como `custom`, se omite este valor.
`quota_memory_limit`	Especifique la asignación de memoria máxima en MB. El valor `0` indica que el uso de memoria no es limitado.
`quota_memory_reservation`	Especifique la asignación de memoria garantizada en MB.
`quota_memory_reservation_percent`	Especifique la asignación de memoria garantizada como un porcentaje de la memoria real de la instancia. El valor `100` indica que la memoria invitada también está completamente reservada. Este parámetro tiene prioridad sobre el parámetro `memory_reservation`.
`quota_memory_shares_level`	Especifica el nivel de recursos compartidos de memoria asignados. Puede introducir **`custom`** y agregar el parámetro `memory_shares_share` para proporcionar un valor personalizado.
`quota_memory_shares_share`	Especifica el número de recursos compartidos de memoria asignados. Si no se establece el parámetro `memory_shares_level` como `custom`, se omite este valor.
`quota_disk_io_limit`	Especifique la asignación de transacciones de disco máxima en E/S por segundo. El valor `0` indica que las transacciones de disco no son limitadas.
`quota_disk_io_reservation`	Especifique la asignación de transacciones de disco garantizadas en E/S por segundo.
`quota_disk_io_shares_level`	Especifica el nivel de recursos compartidos de transacciones de disco asignados. Puede introducir **`custom`** y agregar el parámetro `disk_io_shares_share` para proporcionar un valor personalizado.
`quota_disk_io_shares_share`	Especifica el número de recursos compartidos de transacciones de disco asignados. Si no se establece el parámetro `disk_io_shares_level` como `custom`, se omite este valor.
`quota_vif_limit`	Especifique la asignación máxima de ancho de banda de la interfaz virtual en Mbps. El valor `0` indica que el ancho de banda de la interfaz virtual no es limitado.

Tabla 9-1. Metadatos de imagen en VMware Integrated OpenStack (Continuación)

Especificación adicional	Descripción
`quota_vif_reservation`	Especifique la asignación garantizada de ancho de banda de la interfaz virtual en Mbps.
`quota_vif_shares_level`	Especifica el nivel de recursos compartidos de ancho de banda de la interfaz virtual asignados. Puede introducir **`custom`** y agregar el parámetro `vif_shares_share` para proporcionar un valor personalizado.
`quota_vif_shares_share`	Especifica el número de recursos compartidos de ancho de banda de la interfaz virtual asignados. Si no se establece el parámetro `disk_io_shares_level` como `custom`, se omite este valor.

Copia de seguridad y recuperación

10

Puede hacer copias de seguridad de la instalación de VMware Integrated OpenStack para asegurarse de que pueda recuperarse de los errores que se produzcan.

Este capítulo incluye los siguientes temas:

- Hacer una copia de seguridad de la implementación
- Configurar el servicio de copia de seguridad para almacenamiento en bloque
- Restaurar la implementación desde una copia de seguridad
- Recuperar nodos de OpenStack

Hacer una copia de seguridad de la implementación

Puede hacer copias de seguridad de los datos de servidor de administración, base de datos de OpenStack y archivos de anillo Swift.

Este procedimiento crea una copia de seguridad de los archivos de anillo Swift, pero no realiza copias de seguridad de los objetos almacenados en Swift.

Para obtener información sobre las copias de seguridad de Cinder, consulte Configurar el servicio de copia de seguridad para almacenamiento en bloque.

Requisitos previos

Prepare un servidor NFS para almacenar la información de copia de seguridad.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack.

2 Utilice el comando `viocli backup` para hacer copias de seguridad de la información que desee.

- Ejecute el siguiente comando para hacer una copia de seguridad de los datos del servidor de administración:

  ```
  sudo viocli backup mgmt_server nfs-host-ip:/directory
  ```

  Los archivos de copia de seguridad se almacenan en una carpeta denominada `vio_ms_aaaammddhhmmss`.

- Ejecute el siguiente comando para hacer una copia de seguridad de la base de datos de OpenStack:

  ```
  sudo viocli backup openstack_db nfs-host-ip:/directory
  ```

  Los archivos de copia de seguridad se almacenan en una carpeta denominada `vio_os_db_aaaammddhhmmss`.

- Ejecute el siguiente comando para hacer copias de seguridad del anillo Swift:

  ```
  sudo viocli backup swift_ring nfs-host-ip:/directory
  ```

  Los archivos de copia de seguridad se almacenan en una carpeta denominada `vio_swift_ring_aaaammddhhmmss`.

Pasos siguientes

Si se produce un error en la implementación, puede recuperar nodos individuales o toda la implementación. Para recuperar nodos individuales, consulte Recuperar nodos de OpenStack. Para restaurar la implementación, consulte Restaurar la implementación desde una copia de seguridad.

Configurar el servicio de copia de seguridad para almacenamiento en bloque

La práctica recomendada consiste en configurar un servicio de copia de seguridad para el componente de almacenamiento en bloque (Cinder) de OpenStack a fin de evitar la pérdida de datos. Puede configurar Cinder para realizar copias de seguridad de volúmenes en un servidor de Network File System (NFS).

Para configurar un servicio de copia de seguridad, instale los paquetes Debian de OpenStack que se incluyen en la implementación de VMware Integrated OpenStack.

A los fines de este procedimiento, las dos controladoras se denominan controller01 y controller02.

Requisitos previos

- Cree una carpeta de recurso compartido de NFS dedicada para almacenar la copia de seguridad de los datos.

- Verifique que el propietario de la carpeta del recurso compartido de NFS tenga el mismo UID que Cinder en los nodos de la controladora. El UID predeterminado de Cinder es 107. Este valor puede ser diferente en su implementación.

Procedimiento

1 Mediante SSH, inicie sesión en VMware Integrated OpenStack Manager.

2 Implemente el archivo `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

3 Para usar NFS como servicio de copia de seguridad, edite el archivo `/opt/vmware/vio/custom/custom.yml`.

a Quite la marca de comentario del parámetro `cinder_backup_driver`.

b Establezca el parámetro `cinder_backup_driver` como **`cinder.backup.drivers.nfs`**.

```
# Driver to use for backups. (string value)
cinder_backup_driver: cinder.backup.drivers.nfs
```

c Quite la marca de comentario del parámetro `cinder_backup_share`.

d Establezca el parámetro `cinder_backup_share` como **<dirección IP de host NFS>:<ruta de acceso de copia de seguridad de archivo>**.

```
# NFS share in fqdn:path, ipv4addr:path, or "[ipv6addr]:path"
# format. (string value)
cinder_backup_share: <NFS host IP address>:<file backup path>
```

e Si el recurso compartido de NFS no coincide con su versión de la implementación de VMware Integrated OpenStack, quite la marca de comentario del parámetro `cinder_backup_mount_options` y establézcalo como su versión de NFS.

```
# Mount options passed to the NFS client. See NFS man page for
# details. (string value) 'vers=4' to support version NFS 4
cinder_backup_mount_options: vers=4
```

4 Guarde el archivo `custom.yml`.

5 Inserte la nueva configuración a la implementación de VMware Integrated OpenStack.

```
viocli deployment configure ––limit controller
```

Importante Este comando actualiza toda la implementación y puede que las operaciones se interrumpan brevemente.

6 Verifique que el servicio de copia de seguridad funcione.

a Confirme que el servicio de copia de seguridad de Cinder esté en ejecución.

```
cinder service-list
```

b Cree un volumen de prueba y haga una copia de seguridad de este.

```
cinder create --display-name testvol
cinder backup-create --display-name testvol-backup testvol
```

c Compruebe el recurso compartido de NFS para confirmar que se creó el archivo de copia de seguridad.

Restaurar la implementación desde una copia de seguridad

Es posible restaurar el servidor de administración de VMware Integrated OpenStack y la base de datos de OpenStack desde una copia de seguridad.

Si desea recuperar nodos individuales, consulte Recuperar nodos de OpenStack.

Requisitos previos

Compruebe que exista una copia de seguridad disponible del servidor de administración y de la base de datos. Consulte Hacer una copia de seguridad de la implementación.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Restaure los datos de Servidor de administración de OpenStack.

```
sudo viocli restore mgmt_server backup-folder nfs-host-ip
```

Opción	Descripción
backup-folder	Introduzca el nombre de la carpeta de copia de seguridad para los datos de Servidor de administración de OpenStack. Estas carpetas tienen el formato `vio_ms_aaaammddhhmmss`.
nfs-host-ip	Especifique la dirección IP del host NFS donde se encuentra la carpeta de copia de seguridad.

3 Restaure la base de datos de OpenStack.

```
sudo viocli restore openstack_db backup-folder nfs-host-ip
```

Opción	Descripción
backup-folder	Introduzca el nombre de la carpeta con la copia de seguridad de la base de datos de OpenStack. Estas carpetas tienen el formato `vio_os_db_`*`aaaammddhhmmss`*.
nfs-host-ip	Especifique la dirección IP del host NFS donde se encuentra la carpeta de copia de seguridad.

Servidor de administración de OpenStack y la base de datos de OpenStack se restauran al estado de las copias de seguridad.

Recuperar nodos de OpenStack

En caso de que se produzcan errores de disco u otros problemas críticos, puede recuperar los nodos individuales de la implementación de VMware Integrated OpenStack a través de la interfaz de línea de comandos.

Cuando se recupera un nodo de VMware Integrated OpenStack, este regresa al estado de un nodo recién implementado.

Requisitos previos

- Si desea recuperar todos los nodos de base de datos, debe tener una copia de seguridad de la base de datos de OpenStack. Si desea recuperar nodos Swift, debe tener una copia de seguridad del anillo Swift. Consulte Hacer una copia de seguridad de la implementación.
- Asegúrese de que el almacén de datos tenga suficiente espacio disponible para contener los nodos originales y recuperados al mismo tiempo. El proceso de recuperación elimina el nodo original, pero se requiere espacio para los dos nodos temporalmente. Para evitar este problema, puede apagar y eliminar el nodo existente antes de recuperarlo.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Recupere los nodos de OpenStack por nodo o por función.

Para mostrar los nodos en la implementación, use el comando `viocli show`. Los valores que aparecen en las columnas **Nombre de la máquina virtual** y **Función** pueden utilizarse para recuperar nodos.

a Para recuperar un nodo que no sea de base de datos, ejecute el siguiente comando:

```
sudo viocli recover {–n node1... | –r role1... [–n node1...]}
```

Opción	Descripción
–n	Introduzca los nombres de los nodos que desee recuperar.
–r	Introduzca los nombres de las funciones que desee recuperar. Se recuperarán todos los nodos asignados a la función especificada. Puede especificar `–n` además de este parámetro para recuperar nodos individuales fuera de la función especificada.

b Para recuperar un nodo de base de datos, ejecute el siguiente comando:

```
sudo viocli recover {–n node1... | –r role} –dn backup–name –nfs nfs–host:/backup–folder
```

Opción	Descripción
–n	Introduzca los nombres de los nodos de base de datos que desee recuperar. Puede especificar nodos de `DB` para las implementaciones de HA, o el nodo de `ControlPlane` para las implementaciones compactas o muy pequeñas.
–r	Especifique `DB` para las implementaciones de HA o `ControlPlane` para las implementaciones compactas o muy pequeñas. Se recuperarán todos los nodos de base de datos.

Opción	Descripción
–dn	Introduzca la carpeta que contiene la copia de seguridad de la base de datos de OpenStack. Las carpetas de copias de seguridad de bases de datos de OpenStack tienen el formato `vio_os_db_`*`aaaammddhhmmss`*.
–nfs	Especifique el host NFS y el directorio en el que se encuentra la copia de seguridad con el formato *`remote–host`*`:`*`/remote–dir`*.

c Para recuperar un nodo Swift, ejecute el siguiente comando:

```
sudo viocli recover –n node–name –dn backup–name –nfs nfs–host:/backup–folder
```

Opción	Descripción
–n	Introduzca el nombre de un único nodo Swift.
–dn	Introduzca la carpeta que contiene la copia de seguridad del anillo Swift. Las carpetas de copias de seguridad de Swift tienen el formato `vio_swift_ring_`*`aaaammddhhmmss`*.
–nfs	Especifique el host NFS y el directorio en el que se encuentra la copia de seguridad con el formato *`remote–host`*`:`*`/remote–dir`*.

Importante No se pueden recuperar nodos Swift por función o en lotes. Para evitar la pérdida de datos, compruebe que el nodo recuperado se encuentre en estado operativo y que la replicación de datos al nodo recuperado se haya completado antes de recuperar otros nodos Swift.

El proceso de recuperación puede demorar varios minutos. Para comprobar el estado del nodo, revise la implementación de OpenStack en vSphere Client.

Solucionar problemas en VMware Integrated OpenStack 11

Si se producen errores, es posible realizar acciones de solución de problemas para restaurar la implementación de OpenStack al estado operativo.

Este capítulo incluye los siguientes temas:

Ubicaciones de archivos de registro de VMware Integrated OpenStack

Al solicitar soporte técnico, puede que se le solicite proporcionar archivos de registro. En las siguientes tablas se muestra la ubicación de los archivos y se describe su propósito.

Tabla 11-1. Registros de Servidor de administración de OpenStack

Nombre de archivo	Descripción
`/var/log/apache2/access.log`	Registro del acceso a VMware Integrated OpenStack Manager.
`/var/log/apache2/error.log`	Registro de los errores de acceso de VMware Integrated OpenStack Manager.
`/var/log/column/ansible.log`	Registro de la actividad de servicio de Ansible.
`/var/log/jarvis/jarvis.log`	Registro de la actividad de servicio de Jarvis.
`/var/log/jarvis/pecan.log`	Registro de la actividad de servicio del marco de Pecan.
`/var/log/oms/oms.log`	Registro de la actividad de servicio de VMware Integrated OpenStack Manager.

Tabla 11-1. Registros de Servidor de administración de OpenStack (Continuación)

Nombre de archivo	Descripción
/var/log/oms/register-plugin.log	Registro de la actividad de registro de los complementos de VMware Integrated OpenStack.
/var/log/osvmw/osvmw-exceptions.log	Registro de las excepciones del servicio de osvmw.
/var/log/osvmw/osvmw.log	Registro de la actividad de servicio de osvmw.
/var/log/viocli/viocli.log	Registro de la actividad de servicio de viocli (CLI de VMware Integrated OpenStack).
/var/log/viomon/viomon.log	Registro de la actividad de supervisión de VMware Integrated OpenStack.
/var/log/viopatch/*.log	Registro de la actividad de actualización y revisión.
/var/log/bootsequence.log	Registro de la actividad de arranque.

Tabla 11-2. Registros de controlador

Nombre de archivo	Descripción
/var/log/apache2/access.log	Registra la actividad de acceso al panel de control de VMware Integrated OpenStack.
/var/log/apache2/error.log	Registro de la actividad general de Horizon (panel de control de VMware Integrated OpenStack).
/var/log/atop/atop_*<AAAAMMDD>*	En la parte superior se encuentra la herramienta de supervisión de recursos de OpenStack. El uso de recursos como CPU, memoria y disco se muestrea cada 60 segundos, y los registros se almacenan en un directorio con la fecha en formato AAAAMMDD. Los archivos se rotan cada 3 días de forma predeterminada.
/var/log/cinder/cinder-api.log	Registro de la actividad de servicio de la API de Cinder.
/var/log/cinder/cinder-scheduler.log	Registro de la actividad de servicio del programador de Cinder.
/var/log/cinder/cinder-volume.log	Registro de la actividad de servicio de los volúmenes Cinder.
/var/log/glance/glance-api.log	Registro de la actividad de servicio de la API de Glance.
/var/log/glance/glance-registry.log	Registro de la actividad de servicio del registro de Glance.
/var/log/glance/manage.log	Registro de la actividad general de servicio de Glance.
/var/log/heat/heat-api.log	Registro de la actividad de servicio de la API de Heat.
/var/log/heat/heat-api-cfn.log	Registro de la actividad general de servicio de Heat.
/var/log/heat/heat-api-cloudwatch.log	Registro de la actividad general de servicio de Heat.
/var/log/heat/heat-engine.log	Registro de la actividad de servicio del motor de Heat.
/var/log/keystone/keystone.log	Registro de la actividad general de servicio de Keystone.
/var/log/keystone/keystone-manage.log	Registro de la actividad de servicio de administración de Keystone.
/var/log/neutron/neutron-server.log	Registro de la actividad de servicio de los servidores de Neutron.
/var/log/nova/nova-api.log	Registro de la actividad de servicio de la API de Nova.

Tabla 11-2. Registros de controlador (Continuación)

Nombre de archivo	Descripción
`/var/log/nova/nova-conductor.log`	Registro de la actividad de servicio del conductor de Nova.
`/var/log/nova/nova-consoleauth.log`	Registro de la actividad de servicio de consoleauth de Nova.
`/var/log/nova/nova-manage.log`	Registro de la actividad de servicio de administración de Nova.
`/var/log/nova/nova-mksproxy.log`	Registro de la actividad de servicio de mksproxy de Nova.
`/var/log/nova/nova-novncproxy.log`	Registro de la actividad de servicio de novncproxy de Nova.
`/var/log/nova/nova-scheduler.log`	Registro de la actividad de servicio del programador de Nova.

Tabla 11-3. Registros de base de datos

Nombre de archivo	Descripción
`/var/log/rabbitmq/rabbit@database01.log`	Registro de la actividad de base de datos general de RabbitMQ.
`/var/log/rabbitmq/shutdown_log`	Registro de la actividad de desconexión del servicio de RabbitMQ.
`/var/log/rabbitmq/startup_log`	Registro de la actividad de inicio del servicio de RabbitMQ.
`/var/log/syslog`	Registro de base de datos general, incluido el registro de MySQL.

Tabla 11-4. Registros de procesos

Nombre de archivo	Descripción
`/var/log/ceilometer/ceilometer-agent-compute.log`	Registro de la actividad del agente de Ceilometer.
`/var/log/nova/nova-compute.log`	Registro de la actividad de servicio de proceso para Nova.
`/var/log/nova/nova-manage.log`	Registro de la actividad de servicio del administrador de Nova.
`/var/log/nova/vmware-vspc.log`	Registra la actividad de VMware Virtual Serial Port Concentrator (VSPC).

Tabla 11-5. Registros de equilibrador de carga

Nombre de archivo	Descripción
`/var/log/haproxy/haproxy.log`	Registro de la actividad de servicio de HAProxy.

Ajuste de rendimiento de VMware Integrated OpenStack

Si se deteriora el rendimiento de la implementación de VMware Integrated OpenStack, puede ajustar la configuración de varios componentes de VMware Integrated OpenStack.

Debido a que VMware Integrated OpenStack se implementa en muchos entornos diferentes, no se proporcionan valores recomendados para los parámetros de rendimiento. Ajuste estos parámetros en función de su entorno y los recursos que tenga disponibles.

Los parámetros de la siguiente tabla se encuentran en el archivo `custom.yml`. Debe ejecutar el comando `viocli deployment configure` para que los cambios surtan efecto.

Tabla 11-6. Parámetros de ajuste de rendimiento de VMware Integrated OpenStack

Nombre	Valor predeterminado	Descripción	Uso
`nova_rpc_thread_pool_size`	100	Número máximo de subprocesos simultáneos para Nova	Aumente estos valores para hacer frente a una carga pesada en el proceso para Nova.
`cinder_rpc_thread_pool_size`	100	Número máximo de subprocesos simultáneos para Cinder	
`nova_rpc_response_timeout`	120	Tiempo en segundos durante el que Nova espera una respuesta de una llamada a procedimiento remoto	Aumente estos valores para solucionar el siguiente error en `nova-api.log`: `MessagingTimeout: Timed out waiting for a reply to message ID`
`cinder_rpc_response_timeout`	60	Tiempo en segundos durante el que Cinder espera una respuesta de una llamada a procedimiento remoto	
`nova_max_pool_size`	50	Número máximo de conexiones por grupo de conexión de SQL para Nova	Aumente el valor para solucionar el siguiente error en `nova-api.log`: `TimeoutError: QueuePool limit of size <number> overflow <number> reached, connection timed out`
`cinder_max_pool_size`	5	Número máximo de conexiones por grupo de conexión de SQL para Cinder	
`nova_ram_allocation_ratio`	1,5	Relación de asignación de memoria virtual a la memoria física para filtros de CPU	Aumente el valor para solucionar el siguiente error en `nova-placement-api.log`: `InvalidAllocationCapacityExceeded: Unable to create allocation for 'MEMORY_MB' on resource provider`
`nova_cpu_allocation_ratio`	16	Relación de asignación de CPU virtuales a las CPU físicas para filtros de CPU	Aumente el valor para solucionar el siguiente error en `nova-placement-api.log`: `InvalidAllocationCapacityExceeded: Unable to create allocation for 'VCPU' on resource provider`

Tabla 11-6. Parámetros de ajuste de rendimiento de VMware Integrated OpenStack (Continuación)

Nombre	Valor predeterminado	Descripción	Uso
nova_disk_allocation_ratio	0,0	Relación de asignación de espacio de disco virtual para el espacio de disco físico para los filtros del disco	Aumente el valor para solucionar el siguiente error en nova-placement-api.log: `InvalidAllocationCapacityExceeded: Unable to create allocation for 'DISK_GB' on resource provider`
keystone_token_expiration_time	7200	Tiempo en segundos que un token sigue siendo válido	Aumente el valor para solucionar el siguiente error en varios archivos de registro: `WARNING keystoneclient.middleware.auth_token [-] Authorization failed for token`
haproxy_nova_compute_client_timeout	1200s	Tiempo en segundos que el equilibrador de carga espera una respuesta de Nova como cliente	Aumente estos valores para solucionar el siguiente error en nova-compute.log: `Exception during message handling: Gateway Time-out (HTTP 504)`
haproxy_nova_compute_server_timeout	1200s	Tiempo en segundos que el equilibrador de carga espera una respuesta de Nova como servidor	
haproxy_cinder_client_lb_timeout	300s	Tiempo en segundos que el equilibrador de carga espera una respuesta de Cinder como cliente	Aumente los valores para solucionar el siguiente error en cinder-volume.log: `VolumeBackendAPIException: Bad or unexpected response from the storage volume backend API`
haproxy_cinder_server_lb_timeout	300s	Tiempo en segundos que el equilibrador de carga espera una respuesta de Cinder como servidor	
mysql_max_connections	1000	Número máximo de conexiones globales de MySQL	Aumente el valor para solucionar el siguiente error en nova-compute.log: `Remote error: OperationalError (OperationalError) (1040, 'Too many connections')`

Tabla 11-6. Parámetros de ajuste de rendimiento de VMware Integrated OpenStack (Continuación)

Nombre	Valor predeterminado	Descripción	Uso
`cinder_wsgi_processes`	4	Número máximo de procesos mod_wsgi para Cinder	Aumente estos valores para mejorar el rendimiento y reduzca la aparición de errores HTTP 503 para implementaciones a gran escala con demasiadas operaciones simultáneas.
`cinder_wsgi_threads`	15	Número máximo de subprocesos mod_wsgi para Cinder	
`keystone_wsgi_processes`	8	Número máximo de procesos mod_wsgi para Keystone	
`keystone_wsgi_threads`	15	Número máximo de subprocesos mod_wsgi para Keystone	
`nova_placement_wsgi_processes`	8	Número máximo de procesos mod_wsgi para la colocación de Nova	
`nova_placement_wsgi_threads`	15	Número máximo de subprocesos mod_wsgi para la colocación de Nova	

Mostrar la vApp de VMware Integrated OpenStack

Si la vApp de VMware Integrated OpenStack no se muestra en vSphere, es posible que deba realizar varias acciones.

Problema

VMware Integrated OpenStack se instaló correctamente, pero la vApp no se muestra en vSphere.

Solución

1. En un explorador, abra `https://mgmt-server-ip:8443/VIO` e inicie sesión con las credenciales de administrador para la instancia de vCenter Server.
2. Si el indicador de estado es rojo, siga estos pasos:
   a. Haga clic en **Corregir**.
   b. Verifique el certificado y haga clic en **Aceptar**.
   c. Cierre la sesión de vSphere Client y vuelva a iniciar sesión.
3. Si el problema persiste, confirme que Servidor de administración de OpenStack puede conectarse a la instancia de vCenter Server.
4. Inicie sesión en Servidor de administración de OpenStack y compruebe los registros de la carpeta `/var/log/oms` para confirmar que el servicio de Servidor de administración de OpenStack se inició correctamente.

5 Reinicie el servicio de Servidor de administración de OpenStack.

```
service oms restart
```

6 Cierre la sesión de vSphere Client y vuelva a iniciar sesión.

7 Si el problema persiste, inicie sesión en la máquina virtual de vCenter Server y reinicie el servicio de vSphere Client.

```
service-control --stop vsphere-ui
cd /etc/vmware/vsphere-ui/vc-packages/vsphere-client-serenity/
rm -rf *
cd /usr/lib/vmware-vsphere-client/server/work
rm -rf *
service-control --start vsphere-ui
```

8 Cierre la sesión de vSphere Client y vuelva a iniciar sesión.

Volver a sincronizar las zonas de disponibilidad

En un entorno con varias instancias de vCenter Server, los nombres de las zonas de disponibilidad en el panel de control de VMware Integrated OpenStack pueden diferir de los nombres en Servidor de administración de OpenStack.

Si se utiliza la interfaz de línea de comandos para cambiar el nombre de las zonas de disponibilidad, es posible que se muestren nombres diferentes en vSphere Client y el panel de control de VMware Integrated OpenStack. En la columna **Zonas de disponibilidad** de la pestaña **Administrar > Proceso para Nova** para la implementación, se muestran en rojo las zonas de disponibilidad no sincronizadas. Puede volver a sincronizar las zonas de disponibilidad para solucionar el problema.

Procedimiento

1 Inicie sesión en Servidor de administración de OpenStack y consulte la lista de zonas de disponibilidad de la implementación de OpenStack.

```
sudo viocli inventory-admin show-availability-zones
```

2 Sincronice las zonas de disponibilidad.

```
sudo viocli inventory-admin sync-availability-zones
```

Corregir errores de copia de seguridad de volúmenes Cinder con error de memoria

Cuando se crea una copia de seguridad de un volumen Cinder en un recurso compartido de NFS, se genera un error de memoria.

Problema

Al intentar crear una copia de seguridad de un volumen Cinder, se genera un error de memoria agotada.

Causa

No hay memoria disponible en el controlador.

Solución

1 Implemente el archivo `custom.yml`.

```
sudo mkdir –p /opt/vmware/vio/custom
sudo cp /var/lib/vio/ansible/custom/custom.yml.sample /opt/vmware/vio/custom/custom.yml
```

2 Edite el archivo `/opt/vmware/vio/custom/custom.yml`.

En función de la memoria disponible en el controlador, reduzca el valor del parámetro `cinder_backup_file_size`.

3 Guarde el archivo `custom.yml`.

4 Inserte la nueva configuración a la implementación de VMware Integrated OpenStack.

```
viocli deployment ––verbose configure ––limit controller
```

Corregir errores de copia de seguridad de volúmenes Cinder con errores de permiso denegado

Cuando se intenta crear por primera vez una copia de seguridad de prueba de un volumen Cinder en un recurso compartido de NFS, se genera un error de permiso denegado.

Problema

Al intentar comprobar la configuración de la copia de seguridad de Cinder, se genera un error de permiso al crear la copia de seguridad inicial.

Causa

VMware Integrated OpenStack no tiene los permisos correctos para escribir en el recurso compartido de NFS.

Solución

1 Mediante SSH, inicie sesión en el nodo Controller como usuario raíz.

2 Vaya al directorio de montaje en la configuración de la copia de seguridad de Cinder.

```
cd /var/lib/cinder/backup_mount/
```

3 Cambie el propietario de la carpeta de `root` a `cinder`.

```
chown –R cinder:cinder *
```

Esta solución corrige la configuración y otorga al componente Cinder permisos para acceder al recurso compartido de NFS.

DCLI no se puede conectar al servidor

Si DCLI no se puede conectar a Servidor de administración de OpenStack, es posible que deba reiniciar el servicio de vAPI.

Problema

Cuando se inicia DCLI, aparece el siguiente mensaje de error:

```
ERROR: No se pudo conectar con el servidor.
```

Causa

DCLI no se puede conectar con el endpoint de vAPI debido a que no se está ejecutando el servicio.

Solución

1 Inicie sesión en Servidor de administración de OpenStack como `viouser`.

2 Verifique el estado del servicio de vAPI.

```
sudo systemctl status vapi
```

El servicio está inactivo.

```
vapi.service – VIO vAPI Loaded: loaded (/etc/systemd/system/vapi.service; disabled; vendor preset:
enabled) Active: inactive (dead)
```

3 Reinicie el servicio.

```
sudo systemctl restart vapi
```

4 Vuelva a verificar el estado del servicio de vAPI.

```
sudo systemctl status vapi
```

El servicio se ha reiniciado.

```
vapi.service – VIO vAPI Loaded: loaded (/etc/systemd/system/vapi.service; disabled; vendor preset:
enabled) Active: active (running) since Wed 2018-06-27 04:46:00 UTC; 1s ago Process: 1983
ExecStartPre=/bin/mkdir -p /var/log/vmware/vapi (code=exited, status=0/SUCCESS) Main PID: 1985
(twistd) CGroup: /system.slice/vapi.service └─1985 /usr/bin/python /usr/bin/twistd --nodaemon --
pidfile= -n web --port=9449 --wsgi vmware.vapi.wsgi.application Jun 27 04:46:00 vio-
oms-01.mgt.sg.lab systemd[1]: Starting VIO vAPI... Jun 27 04:46:00 vio-oms-01.mgt.sg.lab
systemd[1]: Started VIO vAPI. ...
```

Pasos siguientes

Conéctese de nuevo a Servidor de administración de OpenStack.

```
dcli +server https://mgmt-server-ip:8443/api +i
```

Sincronizar el estado de las instancias de Nova

Es posible restablecer las instancias de Nova en el estado SHUTOFF o ERROR que se encuentran encendidas en vCenter Server.

Problema

Una instancia de Nova puede permanecer en el estado ERROR o SHUTOFF incluso después de que se enciende la máquina virtual correspondiente a la instancia en vCenter Server.

Solución

1 Inicie sesión en Servidor de administración de OpenStack.

2 Consulte las instancias de Nova en el estado ERROR o SHUTOFF que se muestran como encendidas en vCenter Server.

```
sudo viocli inventory-admin show-instances --nova-state {ERROR | SHUTOFF} --vc-state poweredOn
```

3 Restablezca las instancias encendidas en el estado ERROR o SHUTOFF.

```
sudo viocli inventory-admin reset-instances-state --nova-state {ERROR | SHUTOFF} --vc-state
poweredOn
```

API de VMware Integrated OpenStack 12

VMware Integrated OpenStack incluye varias API que le ayudarán a implementar y administrar OpenStack.

Este capítulo incluye los siguientes temas:

- Usar las API de Servidor de administración de OpenStack
- Usar las vAPI del centro de datos virtual de tenant

Usar las API de Servidor de administración de OpenStack

VMware Integrated OpenStack incluye las API de RESTful que puede utilizar para implementar y administrar OpenStack.

Antes de usar las API, debe autenticarse con el endpoint de la API de Servidor de administración de OpenStack utilizando las credenciales de administrador de la instancia de vCenter Server. Para autenticarse, realice una solicitud POST a `https://mgmt-server-ip:8443/login` e incluya `username=vcenter-user&password=vcenter-password` en el cuerpo de la solicitud.

Después de la autenticación, podrá acceder a las API hasta que caduque la sesión. Si utiliza un explorador web, antes de poder enviar solicitudes de API, debe aceptar el certificado del servidor para establecer un canal seguro entre dicho explorador y Servidor de administración de OpenStack.

Para obtener más información sobre las API, consulte la referencia de la API de VMware Integrated OpenStack en https://code.vmware.com/apis/448. Si instaló VMware Integrated OpenStack, también puede ver las especificaciones de API en `https://mgmt-server-ip:8443/swagger-ui.html`.

Usar las vAPI del centro de datos virtual de tenant

VMware Integrated OpenStack incluye vAPI que puede utilizar para administrar los centros de datos virtuales de tenant.

Si inició sesión en Servidor de administración de OpenStack, también puede administrar los centros de datos virtuales de tenant mediante Data Center Command-Line Interface (DCLI) o la utilidad `viocli`. Para obtener información sobre la utilidad `viocli`, consulte Comando viocli inventory-admin.

Cuando use las vAPI, debe autenticarse con el endpoint de la vAPI utilizando las credenciales de administrador de la instancia de vCenter Server.

Puede utilizar cualquier cliente HTTP para enviar solicitudes al endpoint de vAPI. Este documento utiliza cURL como ejemplo.

Crear un centro de datos virtual de arrendatario

```
curl -X POST -u vcserver-admin -H "Content-Type: application/json"
   https://mgmt-server-ip:9449/rest/vio/tenant/vdc
   -d '{
      "spec":{
         "compute":"compute-node",
         "display_name":"vdc-name",
         "project_id":"project-uuid",
         "cpu_limit":max-cpu-mhz,
         "cpu_reserve":min-cpu-mhz,
         "mem_limit":max-memory-mb,
         "mem_reserve":min-memory-mb
      }
   }'
```

Los parámetros `cpu_limit`, `cpu_reserve`, `mem_limit` y `mem_reserve` son opcionales.

El identificador del nuevo centro de datos virtual de tenant se devuelve con el formato JSON.

El comando de DCLI equivalente es el siguiente:

```
com vmware vio tenant vdc create --compute compute-node --display-name vdc-name --project-id project-
uuid [--cpu-limit max-cpu-mhz] [--cpu-reserve min-cpu-mhz] [--mem-limit max-memory-mb] [--mem-reserve
min-memory-mb]
```

Actualizar un centro de datos virtual de tenant

```
curl -X PATCH -u vcserver-admin -H "Content-Type: application/json"
   https://mgmt-server-ip:9449/rest/vio/tenant/vdc/tenant-vdc-id
   -d '{
      "spec":{
         "compute":"compute01"
         "cpu_limit":max-cpu-mhz,
         "cpu_reserve":min-cpu-mhz,
         "mem_limit":max-memory-mb,
         "mem_reserve":min-memory-mb
      }
   }'
```

Los parámetros `cpu_limit`, `cpu_reserve`, `mem_limit` y `mem_reserve` son opcionales.

El comando de DCLI equivalente es el siguiente:

```
com vmware vio tenant vdc update --compute compute-node --tvdc-id tenant-vdc-id [--cpu-limit max-cpu-
mhz] [--cpu-reserve min-cpu-mhz] [--mem-limit max-memory-mb] [--mem-reserve min-memory-mb]
```

Enumerar todos los centros de datos virtuales de arrendatario

```
curl –u vcserver–admin https://mgmt–server–ip:9449/rest/vio/tenant/vdc
```

La información se devuelve con el formato JSON.

El comando de DCLI equivalente es el siguiente:

```
com vmware vio tenant vdc list
```

Mostrar información acerca de un centro de datos virtual de tenant

```
curl –u vcserver–admin https://mgmt–server–ip:9449/rest/vio/tenant/vdc/tenant–vdc–id
```

El estado, el identificador de proveedor, el nombre para mostrar y las cuotas del centro de datos virtual de tenant se devuelven con el formato JSON.

El comando de DCLI equivalente es el siguiente:

```
com vmware vio tenant vdc get ––tvdc–id tenant–vdc–id
```

Eliminar un centro de datos virtual de tenant

```
curl –X POST –u vcserver–admin –H "Content–Type: application/json"
   https://mgmt–server–ip:9449/rest/vio/tenant/vdc/tenant–vdc–id?action=delete–tvdc
   –d '{
      "spec":{
         "compute":"compute–node"
      }
   }'
```

El parámetro `compute` es opcional. Si especifica `compute`, el centro de datos virtual de tenant se eliminará solo del nodo informático especificado. Si no especifica `compute`, el centro de datos virtual de tenant se eliminará en todos los nodos informáticos.

El comando de DCLI equivalente es el siguiente:

```
com vmware vio tenant vdc deletetvdc ––tvdc–id tenant–vdc–id [––compute compute–node]
```

Referencia de comandos de VMware Integrated OpenStack

13

VMware Integrated OpenStack incluye la utilidad `viocli` para configurar la implementación y la utilidad `viopatch` para administrar e instalar las revisiones. Puede ejecutar ambas utilidades de línea de comandos en Servidor de administración de OpenStack con `sudo`.

A continuación se describen los parámetros compatibles con `viocli` y `viopatch`. También es posible ejecutar `viocli –h` o `viopatch –h` para mostrar los parámetros admitidos.

Este capítulo incluye los siguientes temas:

Comando viocli backup

Utilice el comando `viocli backup` para crear una copia de seguridad de la implementación de OpenStack. Puede hacer copias de seguridad de datos en el servidor de administración, la base de datos de OpenStack o los archivos de anillo Swift. Un servidor NFS debe estar disponible para poder montar VMware Integrated OpenStack.

El comando `viocli backup` usa la siguiente sintaxis.

```
viocli backup {mgmt_server | openstack_db | swift_ring} [-d NAME] NFS-VOLUME [--verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
NFS-VOLUME	Obligatorio	Nombre o dirección IP del volumen NFS de destino y del directorio con el formato *remote-host*:*remote-dir*. Por ejemplo: `192.168.1.77:/backups`
`--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli backup -h` o `viocli backup --help` para mostrar los parámetros del comando.

- Las copias de seguridad del servidor de administración se crean en un directorio denominado con una marca de tiempo en el formato `vio_ms_`*`aaaammddhhmmss`*.
- Las copias de seguridad de bases de datos de OpenStack se crean en un directorio denominado con una marca de tiempo en el formato `vio_os_db_`*`aaaammddhhmmss`*.
- Las copias de seguridad de anillos Swift se crean en un directorio denominado con una marca de tiempo con el formato `vio_swift_ring_`*`aaaammddhhmmss`*.

Comando viocli barbican

Utilice el comando `viocli barbican` para configurar OpenStack Barbican.

El comando `viocli barbican` usa la siguiente sintaxis.

```
viocli barbican [-d NAME] --secret-store-plugin {simple_crypto | KMIP} --host KMIP-SERVER --port KMIP-PORT --ca-certs CA-CERT-PATH {{--certfile CERT-FILE --keyfile KEY-FILE} | {--user KMIP-USER --password KMIP-PASSWORD}} [--ssl-version {PROTOCOL_SSLv23 | PROTOCOL_TLSv1 | PROTOCOL_TLSv1_1 | PROTOCOL_TLSv1_2}] [--verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`--secret-store-plugin {simple_crypto | KMIP}`	Obligatorio	Complemento que se utilizará para Barbican. Solo se admiten `simple_crypto` y `KMIP`.
`--host` *KMIP-SERVER*	Obligatorio si se utiliza el complemento KMIP	Dirección IP del servidor KMIP.
`--port` *KMIP-PORT*	Obligatorio si se utiliza el complemento KMIP	Puerto para conectarse al servidor KMIP.
`--ca-certs` *CA-CERT-PATH*	Obligatorio si se utiliza el complemento KMIP	Ruta de acceso al archivo de certificado de CA.
`--certfile` *CERT-FILE*	Obligatorio si se utiliza el complemento KMIP y no se especifica un nombre de usuario	Ruta de acceso al archivo de certificado de cliente local. Puede especificar un certificado y una clave, un nombre de usuario y una contraseña, o los cuatro.
`--keyfile` *KEY-FILE*	Obligatorio si se especifica un certificado	Ruta de acceso al archivo de claves de cliente local. Puede especificar un certificado y una clave, un nombre de usuario y una contraseña, o los cuatro.
`--user` *KMIP-USER*	Obligatorio si se utiliza el complemento KMIP y no se especifica un certificado	Nombre de usuario para autenticar con el servidor KMIP. Puede especificar un certificado y una clave, un nombre de usuario y una contraseña, o los cuatro.
`--password` *KMIP-PASSWORD*	Obligatorio si se especifica un nombre de usuario	Contraseña para autenticar con el servidor KMIP. Puede especificar un certificado y una clave, un nombre de usuario y una contraseña, o los cuatro.
`--ssl-version {PROTOCOL_SSLv23 | PROTOCOL_TLSv1 | PROTOCOL_TLSv1_1 | PROTOCOL_TLSv1_2}`	Opcional	Versión de TLS que se utilizará para la autenticación. El valor predeterminado es `PROTOCOL_TLSv1_2`.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli barbican -h` o `viocli barbican --help` para mostrar los parámetros del comando.

Comando viocli certificate

Utilice el comando `viocli certificate` para agregar, eliminar y ver certificados.

Nota Para generar una solicitud de firma del certificado (Certificate Signing Request, CSR) o actualizar un certificado existente, consulte Comando viocli deployment.

El comando `viocli certificate` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`-p` o `--progress`	Opcional	Muestra el progreso de la operación actual.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli certificate -h` o `viocli certificate --help` para mostrar las acciones y los parámetros del comando. También puede utilizar la opción `--help` o `-h` en cualquier acción para mostrar los parámetros de la acción. Por ejemplo, `viocli certificate add -h` muestra los parámetros para la acción `add`.

A continuación, se enumeran las acciones que admite `viocli certificate`.

`viocli certificate add [-d NAME] --name CERT-NAME --cert CERT-FILE [-p] [--verbose]`

Agrega un certificado al almacén de certificados. Los siguientes parámetros adicionales se aplican a la acción `add`.

Parámetro	Obligatorio u opcional	Descripción
`--cert` *CERT-FILE*	Obligatorio	Certificado que desea agregar. El certificado debe tener el formato PEM.
`--name` *CERT-NAME*	Obligatorio	Nombre del certificado.

`viocli certificate remove [-d NAME] --name CERT-NAME [-p] [--verbose]`

Elimina un certificado del almacén de certificados. Los siguientes parámetros adicionales se aplican a la acción `remove`.

Parámetro	Obligatorio u opcional	Descripción
`--name` *CERT-NAME*	Obligatorio	Nombre del certificado.

`viocli certificate list [-d NAME] [--json JSON | -pretty PRETTY] [-p] [--verbose]`

Enumera todos los certificados en el almacén de certificados. Los siguientes parámetros adicionales se aplican a la acción `list`.

Parámetro	Obligatorio u opcional	Descripción
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

`viocli certificate show [-d NAME] --name CERT-NAME [--json JSON | --pretty PRETTY] [-p] [--verbose]`

Muestra información detallada sobre un certificado especificado. Los siguientes parámetros adicionales se aplican a la acción `show`.

Parámetro	Obligatorio u opcional	Descripción
`--name` *CERT-NAME*	Obligatorio	Nombre del certificado.
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

Comando viocli dbverify

Utilice el comando `viocli dbverify` para comprobar si la base de datos de VMware Integrated OpenStack presenta problemas como duplicados o claves ausentes.

El comando `viocli dbverify` usa la siguiente sintaxis.

```
viocli dbverify [-d NAME] [--verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`--verbose`	Opcional	Pasa al modo detallado.

También puede ejecutar `viocli dbverify -h` o `viocli dbverify --help` para mostrar los parámetros del comando.

Comando viocli deployment

Use el comando `viocli deployment` para administrar la implementación de VMware Integrated OpenStack.

El comando `viocli deployment` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`-p` o `--progress`	Opcional	Muestra el progreso de la operación actual.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli deployment -h` o `viocli deployment --help` para mostrar los parámetros del comando. También puede utilizar la opción `--help` o `-h` en cualquier acción para mostrar los parámetros de la acción. Por ejemplo, `viocli deployment configure -h` muestra los parámetros para la acción `configure`.

A continuación, se enumeran las acciones que admite `viocli deployment`.

`viocli deployment start [-d NAME] [-f] [-p] [--verbose]`

Inicia una implementación. Los siguientes parámetros adicionales se aplican a la acción `start`.

Parámetro	Obligatorio u opcional	Descripción
`-f` o `--force`	Opcional	Inicia de manera forzosa una implementación que ya está en ejecución.

`viocli deployment stop [-d NAME] [-p] [--verbose]`

Detiene una implementación.

`viocli deployment pause [-d NAME] [-p] [--verbose]`

Pausa una implementación.

`viocli deployment resume [-d NAME] [-p] [--verbose]`

Reanuda una implementación pausada.

`viocli deployment reset_status [-d NAME] [-p] [--verbose]`

Restablece una implementación al estado de ejecución.

Nota Revise los servicios antes de ejecutar este comando.

`viocli deployment configure [-d NAME] [--limit {controller | compute | db | memcache}] [--tags TAGS] [-p] [--verbose]`

Actualiza toda la configuración para una implementación. Los siguientes parámetros adicionales se aplican a la acción `configure`.

Parámetro	Obligatorio u opcional	Descripción
`--limit {controller | compute | db | memcache}`	Opcional	Actualiza la configuración solo para el componente especificado.
`--tags TAGS`	Opcional	Ejecuta solo las tareas de configuración marcadas con las etiquetas especificadas.

`viocli deployment post-deploy [-d NAME] [-p] [--verbose]`

Actualiza la configuración posterior a la implementación.

`viocli deployment run-custom-playbook [-d NAME] [-p] [--verbose]`

Ejecuta solo la guía de estrategias personalizada de Ansible.

viocli deployment cert-req-create [-d *NAME*] [-c *COUNTRY*] [-s *STATE*] [-l *CITY*] [-o *ORG*] [-u *ORG-UNIT*] [--hostname_list *HOST1*[,*HOST2*...]] [-p] [--verbose]

Crea una solicitud de firma del certificado para enviar a una entidad de certificación. Los siguientes parámetros adicionales se aplican a la acción `cert-req-create`.

Parámetro	Obligatorio u opcional	Descripción
-c *COUNTRY* o --country_name *COUNTRY*	Opcional	Código ISO de dos letras del país en el que se ubica la organización que solicita el certificado. Si no incluye esta opción en el comando, se le solicitará que introduzca un valor.
-s *STATE* o --state_name *STATE*	Opcional	Nombre completo de la provincia o el estado. Si no incluye esta opción en el comando, se le solicitará que introduzca un valor.
-l *CITY* o --locality_name *CITY*	Opcional	Nombre de la ciudad o el pueblo. Si no incluye esta opción en el comando, se le solicitará que introduzca un valor.
-o *ORG* o --organization_name *ORG*	Opcional	Nombre legal de la organización. Si no incluye esta opción en el comando, se le solicitará que introduzca un valor.
-u *ORG-UNIT* o --organization_unit_name *ORG-UNIT*	Opcional	Nombre del departamento o de la unidad organizativa. Si no incluye esta opción en el comando, se le solicitará que introduzca un valor.
--hostname_list *HOST1*[,*HOST2*...]	Opcional	Lista de nombres de host, separados por comas. Si no incluye esta opción en el comando, se le solicitará que introduzca un valor.

viocli deployment cert-update [-d *NAME*] [-f *CERT-PATH*] [-p] [--verbose]

Actualiza el certificado que usa VMware Integrated OpenStack. Los siguientes parámetros adicionales se aplican a la acción `cert-update`.

Parámetro	Obligatorio u opcional	Descripción
-f *CERT-PATH* o --file *CERT-PATH*	Opcional	Ruta de acceso absoluta al archivo de certificado deseado. El certificado debe tener el formato PEM.

viocli deployment getlogs [–d *NAME*] [––node *NODE*] [–nrl] [––recent–logs] [–p] [––verbose]

Obtiene archivos de registro para la implementación actual, incluidos los resultados y los comandos Ansible ejecutados. Los archivos de registro se escriben en `/var/log/viocli/viocli.log` y se rotan cuando alcanzan 100 MB. Solo se mantienen las siete rotaciones más recientes.

Los siguientes parámetros adicionales se aplican a la acción `getlogs`.

Parámetro	Obligatorio u opcional	Descripción
`––node` *NODE*	Opcional	Obtiene archivos de registro solo para los nodos especificados. Se admiten los siguientes valores: ■ `ceilometer` ■ `compute` ■ `controller` ■ `db` ■ `dhcp` ■ `lb` ■ `local` ■ `memcache` ■ `mq` ■ `storage`
`–nrl` o `––non–rollover–log–only`	Opcional	Recopila solo los registros que no se archivaron.
`––recent–logs`	Opcional	Recopila solo el archivo de registro en el que actualmente escribe el proceso del servicio.

viocli deployment default [–d *NAME*] [–p] [––verbose]

Devuelve el nombre de la implementación predeterminada.

viocli deployment status [–d *NAME*] [––period *SECONDS*] [––format {text | json}] [–p] [––verbose]

Evalúa el estado de una implementación en términos de lo siguiente:

- Problemas de sincronización entre el servidor de administración y los nodos de OpenStack
- Conexiones con procesos de OpenStack y recuento de conexiones promedio
- Conexiones de red interrumpidas
- Problemas en la base de datos de OpenStack
- Procesos ausentes

Los siguientes parámetros adicionales se aplican a la acción `status`.

Parámetro	Obligatorio u opcional	Descripción
`--period` *SECONDS*	Opcional	Utiliza únicamente datos del período especificado (en segundos). Por ejemplo, `--period 300` evaluará el estado de la implementación en los últimos 5 minutos.
`--format {text | json}`	Opcional	Genera el informe de estado en el formato especificado. Si no se introduce un valor, se utiliza `text` de forma predeterminada.

Comando viocli ds-migrate-prep

Use el comando `viocli ds-migrate-prep` para preparar un almacén de datos para su mantenimiento. El comando `viocli ds-migrate-prep` le permite garantizar que el almacén de datos especificado en la implementación de VMware Integrated OpenStack no contenga referencias rotas.

El comando `viocli ds-migrate-prep` usa la siguiente sintaxis.

```
viocli ds-migrate-prep [-d NAME] DC_NAME DS_NAME [--verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
DC_NAME	Obligatorio	Especifica un centro de datos por nombre.
DS_NAME	Obligatorio	Especifica un almacén de datos por nombre.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli ds-migrate-prep -h` o `viocli ds-migrate-prep --help` para mostrar los parámetros del comando.

Comando viocli enable-tvd

Utilice el comando `viocli enable-tvd` para agregar compatibilidad con redes de NSX-T Data Center a una implementación de VMware Integrated OpenStack que se implementó con NSX Data Center for vSphere.

Importante Este comando actualizará el archivo `custom.yml` o generará automáticamente un archivo `custom.yml` si el archivo no existe en el entorno. Después de ejecutar el comando `viocli enable-tvd`, no elimine `custom.yml` o se descartará la configuración.

`viocli enable-tvd` configura los siguientes parámetros en el archivo `custom.yml`:

- `nsxv3_default_vlan_tz`
- `nsxv3_api_managers`
- `nsxv3_native_md_proxy`
- `nsxv3_ca_file`
- `nsxv3_default_overlay_tz`
- `neutron_backend`
- `nsxv3_default_tier0_router`
- `nsxv3_insecure`
- `nsxv3_api_username`
- `nsxv3_native_dhcp_profile`

El comando `viocli enable-tvd` usa la siguiente sintaxis.

```
viocli enable-tvd [-d NAME] --nsx-mgr MANAGER-IP --nsx-user USERNAME --nsx-passwd PASSWORD [--nsx-
insecure {true | false}] [--nsx-ca-file CA-FILE] [--nsx-overlay-tz OVERLAY-TZ] [--nsx-vlan-tz VLAN-TZ]
[--nsx-tier0-rt TIER0-ROUTER] [--nsx-dhcp-profile DHCP-PROFILE] [--nsx-md-proxy MD-PROXY] [--verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`--nsx-mgr` *MANAGER-IP*	Obligatorio	Dirección IP de la instancia de NSX Manager de la implementación de NSX-T Data Center.
`--nsx-user` *USERNAME*	Obligatorio	Nombre de usuario del administrador de NSX Manager.
`--nsx-passwd` *PASSWORD*	Obligatorio	Contraseña para el administrador de NSX Manager.
`--nsx-insecure {true | false}`	Opcional	Especifica si se debe comprobar el certificado del servidor de NSX Manager. Si no se incluye esta opción, se utiliza `true` de forma predeterminada.

Parámetro	Obligatorio u opcional	Descripción
`--nsx-ca-file` *-CA-FILE*	Opcional	Archivos de paquete de CA que se utilizarán para comprobar el certificado del servidor de NSX Manager. Esta opción se ignora si incluye la opción `--nsx-insecure true`.
`--nsx-overlay-tz` *OVERLAY-TZ*	Opcional	Nombre o UUID de la zona de transporte de superposición de NSX-T Data Center predeterminada que se emplea para crear redes de Neutron aisladas de túnel.
`--nsx-vlan-tz` *VLAN-TZ*	Opcional	Nombre o UUID de la zona de transporte de VLAN de NSX-T Data Center predeterminada que se emplea para establecer puentes entre las redes de Neutron si no se especificó ninguna red física.
`--nsx-tier0-rt` *TIER0-ROUTER*	Opcional	Nombre o UUID del enrutador de nivel 0 predeterminado que se emplea para conectarse a enrutadores lógicos de nivel 1 y configurar redes externas.
`--nsx-dhcp-profile` *DHCP-PROFILE*	Opcional	Nombre o UUID del perfil de servidor DHCP utilizado para habilitar el servicio DHCP nativo. Debe crear el perfil en NSX-T Data Center antes de utilizar el complemento.
`--nsx-md-proxy` *MD-PROXY*	Opcional	Nombre o UUID del servidor proxy de metadatos utilizado para habilitar el servicio de metadatos nativo. Debe crear el servidor proxy en NSX-T Data Center antes de utilizar el complemento.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

Nota Si no se incluyen los parámetros `--nsx-ca-file`, `--nsx-overlay-tz`, `--nsx-vlan-tz`, `--nsx-tier0-rt`, `--nsx-dhcp-profile` o `--nsx-md-proxy`, el sistema intentará determinar la información correcta de forma automática. Si se produce un error en el comando, vuelva a intentarlo con los parámetros incluidos.

También puede ejecutar `viocli enable-tvd -h` o `viocli enable-tvd --help` para mostrar los parámetros del comando.

Comando viocli epops

Use el comando `viocli epops` para administrar el agente End Point Operations Management.

End Point Operations Management es un componente de VMware vRealize Operations Manager. Para obtener más información, consulte el documento *Ayuda de vRealize Operations Manager* para su versión.

El comando `viocli epops` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no se introduce un valor, se utiliza la implementación actual de forma predeterminada.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli epops -h` o `viocli epops --help` para mostrar los parámetros del comando. También puede utilizar la opción `--help` o `-h` en cualquier acción para mostrar los parámetros de la acción. Por ejemplo, `viocli epops install -h` muestra los parámetros para la acción `install`.

A continuación, se enumeran las acciones que admite `viocli epops`.

`viocli epops install [-d` *NAME*`] -s` *TGZ-FILE* `-c` *PROP-FILE* `[--verbose]`

Instala el agente End Point Operations Management. Los siguientes parámetros adicionales se aplican a la acción `install`.

Parámetro	Obligatorio u opcional	Descripción
`-s` *TGZ-FILE* o `--source` *TGZ-FILE*	Obligatorio	Especifica la ruta de acceso local o la dirección URL al paquete instalador del agente.
`-c` *PROP-FILE* o `--config` *PROP-FILE*	Obligatorio	Especifica la ruta de acceso local para el archivo de configuración del agente.

`viocli epops uninstall [-d` *NAME*`] [--verbose]`

Desinstala el agente End Point Operations Management.

`viocli epops reconfig [-d` *NAME*`] -c` *PROP-FILE* `[--verbose]`

Actualiza la configuración del agente End Point Operations Management. Los siguientes parámetros adicionales se aplican a la acción `reconfig`.

Parámetro	Obligatorio u opcional	Descripción
`-c` *PROP-FILE* o `--config` *PROP-FILE*	Obligatorio	Especifica la ruta de acceso local para el archivo de configuración del agente.

`viocli epops start [–d NAME] [––verbose]`

Inicia el agente End Point Operations Management.

`viocli epops stop [–d NAME] [––verbose]`

Detiene el agente End Point Operations Management.

Comando viocli federation

Utilice el comando `viocli federation` para configurar la identidad federada Keystone en la implementación de VMware Integrated OpenStack.

El comando `viocli federation` puede ejecutar diversas acciones en los metadatos del proveedor de identidad (Identity Provider, IdP), los proveedores de servicios Keystone y los proveedores de identidad Keystone. Los siguientes parámetros se aplican a todas las acciones en todos los componentes.

Parámetro	Obligatorio u opcional	Descripción
`–d` *NAME* o `––deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`–p` o `––progress`	Opcional	Muestra el progreso de la operación actual.
`––verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli federation –h` o `viocli federation ––help` para mostrar los parámetros del comando. También puede utilizar la opción `––help` o `–h` en cualquier componente o acción para mostrar los parámetros pertinentes. Por ejemplo, `viocli federation idp–metadata –h` mostrará los parámetros para el componente `idp–metadata` y `viocli federation idp–metadata set –h` mostrará los parámetros para la acción `set` en ese componente.

Metadatos del proveedor de identidad

A continuación, se enumeran las acciones que admite `viocli federation` para los metadatos del proveedor de identidad.

`viocli federation idp–metadata clear [–d NAME] [–p] [––verbose]`

Elimina los metadatos del proveedor de identidad.

`viocli federation idp-metadata set [-d NAME] [-p] [--verbose]`

Establece los metadatos del proveedor de identidad. Se le solicitará que introduzca la información de la organización y el contacto.

`viocli federation idp-metadata show [-d NAME] [--json JSON | --pretty PRETTY] [-p] [--verbose]`

Muestra los metadatos del proveedor de identidad. Los siguientes parámetros adicionales se aplican a la acción `show`.

Parámetro	Obligatorio u opcional	Descripción
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

Nota Después de actualizar o eliminar metadatos, debe ejecutar el comando `viocli identity configure` para que se apliquen los cambios.

Proveedores de servicios Keystone

A continuación, se enumeran las acciones que admite `viocli federation` para los proveedores de servicios Keystone.

`viocli federation service-provider add [-d NAME] [--type SP-TYPE] [-p] [--verbose]`

Agrega un proveedor de servicios. Se le solicitará que introduzca información de Keystone. Los siguientes parámetros adicionales se aplican a la acción `add`.

Parámetro	Obligatorio u opcional	Descripción
`--type` *SP-TYPE*	Opcional	Especifica el tipo de proveedor de servicios que se desea agregar.

`viocli federation service-provider remove [-d NAME] --id SP-ID [-p] [--verbose]`

Quita un proveedor de servicios. Los siguientes parámetros adicionales se aplican a la acción `remove`.

Parámetro	Obligatorio u opcional	Descripción
`--id` *SP-ID*	Obligatorio	Identificador del proveedor de servicios que se desea eliminar. Puede ejecutar el comando `viocli federation service-provider list` para mostrar el identificador de cada proveedor de servicios.

`viocli federation service-provider edit [-d` *NAME*`] --id` *SP-ID* `[-p] [--verbose]`

Modifica la configuración de un proveedor de servicios. Los siguientes parámetros adicionales se aplican a la acción `edit`.

Parámetro	Obligatorio u opcional	Descripción
`--id` *SP-ID*	Obligatorio	Identificador del proveedor de servicios que se desea modificar. Puede ejecutar el comando `viocli federation service-provider list` para mostrar el identificador de cada proveedor de servicios.

`viocli federation service-provider list [-d` *NAME*`] [--json JSON | --pretty PRETTY] [-p] [--verbose]`

Muestra información sobre todos los proveedores de servicios. Los siguientes parámetros adicionales se aplican a la acción `list`.

Parámetro	Obligatorio u opcional	Descripción
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

`viocli federation service-provider show [-d` *NAME*`] --id` *SP-ID* `[--json JSON | --pretty PRETTY] [-p] [--verbose]`

Muestra información detallada acerca de un proveedor de servicios. Los siguientes parámetros adicionales se aplican a la acción `show`.

Parámetro	Obligatorio u opcional	Descripción
`--id` *SP-ID*	Obligatorio	Identificador del proveedor de servicios.
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

Proveedores de identidad Keystone

A continuación, se enumeran las acciones que admite `viocli federation` para los proveedores de identidades Keystone.

`viocli federation identity-provider add [-d NAME] [--type {keystone | saml2 | vidm | openid}] [-p] [--verbose]`

Agrega un proveedor de servicios. Se le solicitará que introduzca información de Keystone. Los siguientes parámetros adicionales se aplican a la acción `add`.

Parámetro	Obligatorio u opcional	Descripción
`--type {keystone | saml2 | vidm | openid}`	Opcional	Especifica el tipo de proveedor de identidades que se desea agregar. Si no incluye esta opción en el comando, se le solicitará que introduzca un valor.

`viocli federation identity-provider remove [-d NAME] --id IDP-ID [-p] [--verbose]`

Quita un proveedor de identidad. Los siguientes parámetros adicionales se aplican a la acción `remove`.

Parámetro	Obligatorio u opcional	Descripción
`--id` *IDP-ID*	Obligatorio	Identificador del proveedor de identidad que se desea eliminar. Puede ejecutar el comando `viocli federation identity-provider list` para mostrar el identificador de cada proveedor de identidad.

`viocli federation identity-provider edit [-d NAME] --id IDP-ID [-p] [--verbose]`

Modifica la configuración de un proveedor de identidad. Los siguientes parámetros adicionales se aplican a la acción `edit`.

Parámetro	Obligatorio u opcional	Descripción
`--id` *IDP-ID*	Obligatorio	Identificador del proveedor de identidad que se desea modificar. Puede ejecutar el comando `viocli federation identity-provider list` para mostrar el identificador de cada proveedor de identidad.

`viocli federation identity-provider list [-d NAME] [--json JSON | --pretty PRETTY] [-p] [--verbose]`

Muestra información sobre todos los proveedores de identidad. Los siguientes parámetros adicionales se aplican a la acción `list`.

Parámetro	Obligatorio u opcional	Descripción
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

`viocli federation identity-provider show [-d NAME] --id IDP-ID [--json JSON | --pretty PRETTY] [-p] [--verbose]`

Muestra información detallada acerca de un proveedor de identidad. Los siguientes parámetros adicionales se aplican a la acción `show`.

Parámetro	Obligatorio u opcional	Descripción
`--id` *IDP-ID*	Obligatorio	Identificador del proveedor de identidad.
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

Comando viocli identity

Utilice el comando `viocli identity` si desea configurar Keystone para dominios con back-ends de AD o LDAP. El comando llama a la API de Servidor de administración de OpenStack para almacenar conocimiento de los dominios de Keystone y las variables de diccionario.

El comando `viocli identity` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`-p` o `--progress`	Opcional	Muestra el progreso de la operación actual.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli identity –h` o `viocli identity ––help` para mostrar los parámetros del comando. También puede utilizar la opción `––help` o `–h` en cualquier acción para mostrar los parámetros de la acción. Por ejemplo, `viocli identity add –h` muestra los parámetros para la acción `add`.

A continuación, se enumeran las acciones que admite `viocli identity`.

viocli identity add [–d *NAME*] [––type {AD | LDAP}] [–p] [––verbose]

Configura un nuevo origen de identidad. Los siguientes parámetros adicionales se aplican a la acción `add`.

Parámetro	Obligatorio u opcional	Descripción
`––type {AD | LDAP}`	Opcional	Tipo de back-end para el dominio. Si no incluye el parámetro `––type` en el comando, se le solicitará que introduzca el tipo de back-end.

viocli identity remove [–d *NAME*] ––id *DOMAIN* [–p] [––verbose]

Elimina un origen de identidad de la lista. No se pueden quitar el dominio local (identificador `0`) ni el dominio predeterminado (identificador `1`).

Los siguientes parámetros adicionales se aplican a la acción `remove`.

Parámetro	Obligatorio u opcional	Descripción
`––id` *DOMAIN*	Obligatorio	Identificador de un origen de identidad. El dominio local se representa con `0` y el dominio predeterminado con `1`.

viocli identity configure [–d *NAME*] [–p] [––verbose]

Configura los orígenes de identidad para la implementación.

viocli identity edit [–d *NAME*] ––id *DOMAIN* [–p] [––verbose]

Cambia la configuración de un origen de identidad existente. No se puede editar el dominio local (identificador `0`).

Los siguientes parámetros adicionales se aplican a la acción `edit`.

Parámetro	Obligatorio u opcional	Descripción
`--id` *DOMAIN*	Obligatorio	Identificador de un origen de identidad. El dominio local se representa con `0` y el dominio predeterminado con `1`.

`viocli identity list [-d` *NAME*`] [--json JSON | --pretty PRETTY] [-p] [--verbose]`

Muestra todos los dominios configurados con sus números de identificador y tipos de back-end. Los siguientes parámetros adicionales se aplican a la acción `list`.

Parámetro	Obligatorio u opcional	Descripción
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

`viocli identity show [-d` *NAME*`] --id` *DOMAIN* `[--json JSON | --pretty PRETTY] [-p] [--verbose]`

Muestra información detallada sobre el dominio especificado. Los siguientes parámetros adicionales se aplican a la acción `show`.

Parámetro	Obligatorio u opcional	Descripción
`--id` *DOMAIN*	Obligatorio	Identificador de un origen de identidad. El dominio local se representa con `0` y el dominio predeterminado con `1`.
`--json JSON` `--pretty PRETTY`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `PRETTY` cuando se ejecuta el comando de forma interactiva y `JSON` cuando se ejecuta el comando de forma no interactiva.

Comando viocli inventory-admin

Utilice el comando `viocli inventory-admin` para comparar los inventarios de almacenamiento en bloque y de proceso con el inventario de vSphere, así como para detectar y quitar objetos huérfanos, y administrar centros de datos virtuales de tenant.

Los objetos huérfanos se definen de la siguiente manera:

- Las instancias huérfanas de Nova son aquellas para las que no existe una máquina virtual correspondiente en vSphere.
- Las máquinas virtuales huérfanas son aquellas para las que no existe una instancia correspondiente en la base de datos de OpenStack.

- Las máquinas virtuales de sombra huérfanas son aquellas para las que no existe un volumen de Cinder correspondiente en la base de datos de OpenStack.

El comando `viocli inventory-admin` recopila las credenciales de vCenter Server y OpenStack de los inventarios internos. Este comando requiere que el usuario se autentique como un administrador de OpenStack. El dominio y el nombre de usuario de esta cuenta se establecen en `/root/cloudadmin.rc` como las variables `OS_PROJECT_DOMAIN_NAME`, `OS_USERNAME` y `OS_USER_DOMAIN_NAME`. También se puede establecer la contraseña de esta cuenta como la variable de entorno `OS_PASSWORD` para evitar introducir esta contraseña cada vez que se ejecute el comando.

El comando `viocli inventory-admin` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`--json` `--pretty`	Opcional	Muestra los resultados en formato JSON o como texto con formato. Si no se introduce un valor, se utiliza `--pretty` cuando se ejecuta el comando de forma interactiva y `--json` cuando se ejecuta el comando de forma no interactiva.
`--all`	Opcional	Muestra todos los objetos en lugar de solo los objetos huérfanos.
`--force`	Opcional	Ejecuta el comando sin solicitar una confirmación.
`--no-grace-period`	Opcional	Omite el período de gracia al determinar si los objetos son huérfanos. Los objetos modificados en los últimos 30 minutos se incluyen en los resultados solo cuando se establece este parámetro.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli inventory-admin -h` o `viocli inventory-admin --help` para mostrar los parámetros del comando. También puede utilizar la opción `--help` o `-h` en cualquier acción para mostrar los parámetros de la acción. Por ejemplo, `viocli inventory-admin show-instances -h` muestra los parámetros para la acción `show-instances`.

A continuación, se enumeran las acciones que admite `viocli inventory-admin`.

`viocli inventory-admin show-instances [-d NAME] [--nova-state {ERROR | SHUTOFF} [--vc-state {poweredOn | poweredOff | suspended}]] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]`

Enumera las instancias huérfanas de Nova. También puede utilizar los siguientes parámetros adicionales para enumerar las instancias de Nova que se encuentran en el estado especificado.

Parámetro	Obligatorio u opcional	Descripción
`--nova-state {ERROR | SHUTOFF}`	Opcional	Muestra las instancias de Nova en el estado `ERROR` o `SHUTOFF`. Se muestran todas las instancias huérfanas y no huérfanas independientemente del parámetro `--all`.
`--vc-state {poweredOn | poweredOff | suspended}`	Opcional	Muestra las instancias de Nova en el estado especificado que se encuentran encendidas, apagadas o suspendidas en vCenter Server. Si utiliza este parámetro, también debe incluir el parámetro `--nova-state`. Se muestran todas las instancias huérfanas y no huérfanas independientemente del parámetro `--all`.

viocli inventory-admin show-instance-vms [-d *NAME*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Enumera las máquinas virtuales huérfanas de vSphere.

viocli inventory-admin show-shadow-vms [-d *NAME*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Enumera las máquinas virtuales de sombra huérfanas.

viocli inventory-admin clean-instances [-d *NAME*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Elimina las máquinas virtuales huérfanas de vSphere.

viocli inventory-admin clean-instance-vms [-d *NAME*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Elimina las máquinas virtuales huérfanas de vSphere.

viocli inventory-admin clean-shadow-vms [-d *NAME*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Elimina las máquinas virtuales de sombra huérfanas.

viocli inventory-admin reset-instances-state [-d *NAME*] --nova-state {ERROR | SHUTOFF} --vc-state poweredOn [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Restablece las instancias en el estado ERROR o SHUTOFF que se encuentran encendidas en vCenter Server.

Parámetro	Obligatorio u opcional	Descripción
`--nova-state {ERROR | SHUTOFF} --vc-state poweredOn`	Obligatorio	Restablece las instancias de Nova en el estado ERROR o SHUTOFF que se encuentran encendidas en vCenter Server.

viocli inventory-admin show-hypervisors [-d *NAME*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Enumera los hipervisores con información detallada.

viocli inventory-admin show-availability-zones [-d *NAME*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Enumera las zonas de disponibilidad y los hosts que se encuentran en ellas.

viocli inventory-admin sync-availability-zones [-d *NAME*] [--filename *ZONE-MAP*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Sincroniza las zonas de disponibilidad en el entorno con el mapa especificado. Se admiten los siguientes parámetros adicionales.

Parámetro	Obligatorio u opcional	Descripción
`--filename` *ZONE-MAP*	Opcional	Ruta de acceso al archivo que contiene el mapa de zonas de disponibilidad. El archivo debe tener el formato JSON.

viocli inventory-admin create-tenant-vdc [-d *NAME*] --compute *COMPUTE-NODE* --name *VDC-NAME* --project-id *ID* [--cpu-reserve *CPU-MIN*] [--cpu-limit *CPU-MAX*] [--mem-reserve *MEMORY-MIN*] [--mem-limit *MEMORY-MAX*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Crea un centro de datos virtual (Virtual Data Center, VDC) de arrendatario con la configuración especificada. Se admiten los siguientes parámetros adicionales.

Parámetro	Obligatorio u opcional	Descripción
`--compute` *COMPUTE-NODE*	Obligatorio	Nodo informático en el que se creará el VDC.
`--name` *VDC-NAME*	Obligatorio	Nombre del VDC de arrendatario.
`--project-id` *ID*	Obligatorio	Identificador de proyecto para la tarea.
`--cpu-reserve` *CPU-MIN*	Opcional	Ciclos de CPU en MHz que se reservarán para el VDC. Si no se introduce un valor, se utiliza `0` de forma predeterminada.
`--cpu-limit` *CPU-MAX*	Opcional	Límite máximo para el uso de CPU en el VDC (en MHz). Si no introduce un valor, el uso de CPU no es limitado.
`--mem-reserve` *MEMORY-MIN*	Opcional	Memoria en megabytes que se reservará para el VDC. Si no se introduce un valor, se utiliza `0` de forma predeterminada.
`--mem-limit` *MEMORY-MAX*	Opcional	Límite máximo para el uso de memoria en el VDC (en megabytes). Si no introduce un valor, el uso de memoria no es limitado.

viocli inventory-admin list-tenant-vdcs [-d *NAME*] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Enumera los VDC de arrendatario.

viocli inventory-admin show-tenant-vdc [-d *NAME*] --id *ID* [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]

Muestra información detallada sobre el VDC de arrendatario especificado. Se admiten los siguientes parámetros adicionales.

Parámetro	Obligatorio u opcional	Descripción
`--id` *ID*	Obligatorio	Identificador de un VDC de arrendatario.

`viocli inventory-admin delete-tenant-vdc [-d NAME] --id ID [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]`

Elimina el VDC de arrendatario especificado. Se admiten los siguientes parámetros adicionales.

Parámetro	Obligatorio u opcional	Descripción
`--id` *ID*	Obligatorio	Identificador de un VDC de arrendatario.
`--compute` *COMPUTE-NODE*	Opcional	Nodo informático del que se eliminará el VDC. Si no introduce ningún valor, el VDC se eliminará de todos los nodos informáticos.

`viocli inventory-admin update-tenant-vdc [-d NAME] --compute COMPUTE-NODE --name VDC-NAME --project-id ID [--cpu-reserve CPU-MIN] [--cpu-limit CPU-MAX] [--mem-reserve MEMORY-MIN] [--mem-limit MEMORY-MAX] [--json | --pretty] [--all] [--force] [--no-grace-period] [--verbose]`

Actualiza la configuración del VDC de arrendatario especificado. Se admiten los siguientes parámetros adicionales.

Parámetro	Obligatorio u opcional	Descripción
`--compute` *COMPUTE-NODE*	Obligatorio	Nodo informático donde se ejecuta el VDC.
`--id` *VDC-ID*	Obligatorio	Identificador del VDC de arrendatario.
`--cpu-reserve` *CPU-MIN*	Opcional	Ciclos de CPU en MHz que se reservarán para el VDC.
`--cpu-limit` *CPU-MAX*	Opcional	Límite máximo para el uso de CPU en el VDC (en MHz). El valor –1 indica que el uso de CPU no es limitado.
`--mem-reserve` *MEMORY-MIN*	Opcional	Memoria en megabytes que se reservará para el VDC.
`--mem-limit` *MEMORY-MAX*	Opcional	Límite máximo para el uso de memoria en el VDC (en megabytes). El valor –1 indica que el uso de memoria no es limitado.

Comando viocli lbaasv2-enable

El comando `viocli lbaasv2-enable` ya no es compatible.

Para habilitar LBaaS a través de la interfaz de línea de comandos, consulte "Configurar LBaaS con la interfaz de la línea de comandos" en la *Guía de usuario de VMware Integrated OpenStack*.

Comando viocli recover

Use el comando `viocli recover` para recuperar nodos o grupos de nodos.

Como la mayoría de los nodos de OpenStack no tienen estado, es posible recuperarlos sin un archivo de copia de seguridad. Sin embargo, se necesita un archivo de copia de seguridad para recuperar los nodos de base de datos de OpenStack o los nodos Swift.

El comando `viocli recover` usa la siguiente sintaxis.

```
viocli recover [–d NAME] {–n NODE1... | –r ROLE1... [–n NODE1...]} [–dn BACKUP] [–nfs NFS–VOLUME] [––verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`–d` *NAME* o `––deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`–n, ––node` *NODE*	Obligatorio a menos que se utilice `–r`	Recupera uno o varios nodos. Puede especificar varios nodos, separados por comas. Para mostrar los nodos en la implementación, use el comando `viocli show`. Los valores que se muestran en la columna **Nombre de la máquina virtual** pueden utilizarse como argumentos para este comando. Por ejemplo, el siguiente comando recupera los dos nodos del archivo de copia de seguridad de NFS especificado. `viocli recover –n VIO–DB–0 VIO–DB–1 –dn vio_os_db_20150830215406 –nfs 10.146.29.123:/backups`
`–r` *ROLE* o `––role` *ROLE*	Obligatorio a menos que se utilice `–n`	Recupera todos los nodos asignados a la función especificada. Puede especificar varias funciones, separadas por comas. También puede especificar `–n` o `––node` en el mismo comando para recuperar nodos adicionales no asignados a esa función. Para mostrar los nodos en la implementación, use el comando `viocli show`. Los valores que se muestran en la columna **Función** pueden utilizarse como argumentos para este comando. **Nota** No se pueden recuperar nodos Swift por función. Por ejemplo, el siguiente comando recupera los nodos asignados a la función BD del archivo de copia de seguridad de NFS especificado. `viocli recover –r DB –dn vio_os_db_20150830215406 –nfs 10.146.29.123:/backups`
`–dn` *BACKUP* o `––dir–name` *BACKUP*	Obligatorio para la recuperación de un nodo Swift o la recuperación completa de una base de datos de OpenStack	Carpeta que contiene los archivos de copia de seguridad de la base de datos de OpenStack o del anillo Swift. ■ Las carpetas de copias de seguridad de bases de datos de OpenStack tienen el formato `vio_os_db_`*aaaammddhhmmss*. ■ Las carpetas de copias de seguridad del anillo Swift tienen el formato `vio_swift_ring_`*aaaammddhhmmss*. Este parámetro es obligatorio cuando se recuperan los siguientes elementos: ■ Para una implementación de HA: la función `DB` o los tres nodos de base de datos (`VIO–DB–0`, `VIO–DB–1` y `VIO–DB–2`) ■ Para una implementación compacta o muy pequeña: la función `ControlPlane` o el nodo `VIO–ControlPlane–0` ■ Nodos Swift

Parámetro	Obligatorio u opcional	Descripción
`–nfs` *NFS-VOLUME*	Obligatorio para la recuperación de un nodo Swift o la recuperación completa de una base de datos de OpenStack	Nombre o dirección IP del volumen NFS de destino y del directorio con el formato *remote-host*:*remote-dir*. Por ejemplo: `192.168.1.77:/backups` Este parámetro es obligatorio cuando se recuperan los siguientes elementos: ■ Para una implementación de HA: la función `DB` o los tres nodos de base de datos (`VIO–DB–0`, `VIO–DB–1` y `VIO–DB–2`) ■ Para una implementación compacta o muy pequeña: la función `ControlPlane` o el nodo `VIO–ControlPlane–0` ■ Nodos Swift
`––verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli recover –h` o `viocli recover ––help` para mostrar los parámetros del comando.

Comando viocli restore

Use el comando `viocli restore` para restaurar una implementación desde un archivo de copia de seguridad creado previamente mediante el comando `viocli backup`. Puede restaurar una copia de seguridad de los datos del servidor de administración o de la base de datos de OpenStack.

El comando `viocli restore` usa la siguiente sintaxis.

```
viocli restore {mgmt_server | openstack_db} [–d NAME] DIR–NAME NFS–VOLUME [––verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`–d` *NAME* o `––deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
DIR-NAME	Obligatorio	Directorio que contiene el archivo de copia de seguridad.
NFS-VOLUME	Obligatorio	Nombre o dirección IP del volumen NFS de destino y del directorio con el formato *remote-host*:*remote-dir*. Por ejemplo: `192.168.1.77:/backups`
`––verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli restore –h` o `viocli restore ––help` para mostrar los parámetros del comando.

El archivo de copia de seguridad para el servidor de administración de VMware Integrated OpenStack se etiqueta con una marca de tiempo en el formato `vio_ms_`*`aaaammddhhmmss`*. El archivo de copia de seguridad de la base de datos de VMware Integrated OpenStack se etiqueta con una marca de tiempo en el formato `vio_os_db_`*`aaaammddhhmmss`*.

Comando viocli rollback

El comando `viocli rollback` ya no es compatible.

Para revertir una revisión reciente, consulte "Revertir una revisión de VMware Integrated OpenStack" en *Guía de instalación y configuración de VMware Integrated OpenStack*.

Para revertir desde una actualización reciente, consulte "Revertir a una implementación anterior de VMware Integrated OpenStack" en *Guía de instalación y configuración de VMware Integrated OpenStack*.

Comando viocli services

Use el comando `viocli services` para iniciar o detener todos los servicios de OpenStack.

El comando `viocli services stop` solo detiene los servicios que se ejecutan en su implementación. Para detener el clúster completo, incluidas las máquinas virtuales, ejecute el comando `viocli deployment stop` en su lugar.

El comando `viocli services` usa la siguiente sintaxis.

```
viocli services [-d NAME] {start | stop} [--verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli services -h` o `viocli services --help` para mostrar los parámetros del comando.

Comando viocli show

Use el comando `viocli show` para mostrar una lista de los nodos de una implementación de VMware Integrated OpenStack, o bien para obtener información detallada sobre el inventario de la implementación.

El comando `viocli show` usa la siguiente sintaxis.

```
viocli show [-d NAME] [-i | -p]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`-i` o `--inventory`	Opcional	Muestra el contenido del archivo de inventario para la implementación actual.
`-p` o `--inventory-path`	Opcional	Muestra la ruta de acceso al archivo de inventario para la implementación actual.

Para obtener una lista de nodos, ejecute `viocli show` sin las opciones `-p` o `-i`.

También puede ejecutar `viocli show -h` o `viocli show --help` para mostrar los parámetros del comando.

Comando viocli swift

Utilice el comando `viocli swift` para administrar clústeres y nodos de Swift en la implementación de OpenStack.

El comando `viocli swift` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`-p` o `--progress`	Opcional	Muestra el progreso de la operación actual.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli swift -h` o `viocli swift --help` para mostrar los parámetros del comando. También puede utilizar la opción `--help` o `-h` en cualquier acción para mostrar los parámetros de la acción. Por ejemplo, `viocli swift create-cluster -h` muestra los parámetros para la acción `create-cluster`.

A continuación, se enumeran las acciones que admite `viocli swift`.

`viocli swift create-cluster [-d` *NAME*`] --cluster-moid` *MOID* `--datastores` *DS1*`[,`*DS2*`...] [--storage-node-count` *STORAGE-NODES*`] [--proxy-node-count` *PROXY-NODES*`] [--disk-size` *GB*`] [--swift-partition-power-count` *PARTITION-POWER*`] [--swift-replica-count` *REPLICAS*`] [--swift-min-part-hours` *HOURS*`] [-f` *SPEC-FILE*`] [-p] [--verbose]`

Crea un clúster de Swift. Los siguientes parámetros adicionales se aplican a la acción `create-cluster`.

Parámetro	Obligatorio u opcional	Descripción
`--cluster-moid`	Obligatorio a menos que se utilice `-f`	Identificador de objeto administrado (Managed Object ID, MOID) del clúster de vSphere.
`--datastores`	Obligatorio a menos que se utilice `-f`	Almacenes de datos que se utilizarán para los nodos de almacenamiento de Swift, separados por comas. **Importante** Swift no admite clústeres de almacenes de datos.
`--storage-node-count`	Opcional	Cantidad de nodos de almacenamiento de Swift que se crearán. Si no se introduce un valor, se utiliza `3` de forma predeterminada.
`--proxy-node-count`	Opcional	Cantidad de nodos de proxy de Swift que se crearán. Si no se introduce un valor, se utiliza `2` de forma predeterminada.
`--disk-size`	Opcional	Tamaño de disco en gigabytes para los nodos de almacenamiento de Swift. Si no se introduce un valor, se utiliza `2048` de forma predeterminada.
`--swift-partition-power-count`	Opcional	Alimentación de la partición del anillo Swift. El número de particiones que administra el anillo es igual a 2 elevado a la alimentación de partición. Si no se introduce un valor, se utiliza `10` de forma predeterminada.
`--swift-replica-count`	Opcional	Número de réplicas que se crearán para los objetos que se almacenan en Swift. Si no se introduce un valor, se utiliza `3` de forma predeterminada. **Nota** El número de réplicas no puede superar el número de nodos de almacenamiento en la implementación.
`--swift-min-part-hours`	Opcional	Tiempo en horas antes de que pueda asignarse una partición a otro nodo de almacenamiento. Si no se introduce un valor, se utiliza `1` de forma predeterminada.
`-f` o `--json-file`	Opcional	Archivo JSON que contiene los parámetros para crear el clúster de Swift.

El formato del archivo JSON es el siguiente:

```
{
        "cluster_moid": "moid",
        "storage_node_number": storage-nodes,
        "proxy_node_number": proxy-nodes,
        "ring_settings": {
                "swift_replica_count": replicas,
                "swift_min_part_hours": hours,
                "swift_partition_power_count": power
        },
        "storage_settings": [
                {
                        "datastore_name": "ds1",
                        "zone_number": ds1-zone,
                        "disk_size": ds1-disk-gb
                }
        ]
}
```

Cree una copia del contenido de la sección `storage_settings` para cada nodo de almacenamiento que desee crear.

Si no usa un archivo JSON para crear el clúster, los números de zona se asignarán a los almacenes de datos especificados en orden. Puede usar el parámetro `zone_number` en el archivo JSON para asignar números de zona específicos o para colocar varios almacenes de datos en la misma zona. Un solo almacén de datos no puede ubicarse en varias zonas.

viocli swift delete-cluster [-d *NAME*] [-f] [-p] [--verbose]

Elimina el clúster de Swift.

Parámetro	Obligatorio u opcional	Descripción
`-f` o `--force`	Opcional	Elimina el clúster sin solicitar una confirmación.

viocli swift add-storage [-d *NAME*] --datastores *DS1*[,*DS2*...] [--storage-node-count *STORAGE-NODES*] [--disk-size *GB*] [-f *SPEC-FILE*] [-p] [--verbose]

Agrega nodos de almacenamiento a un clúster de Swift existente.

Parámetro	Obligatorio u opcional	Descripción
`--datastores`	Obligatorio a menos que se utilice `-f`	Almacenes de datos que se utilizarán para los nuevos nodos de almacenamiento de Swift, separados por comas. **Importante** Swift no admite clústeres de almacenes de datos.
`--storage-node-count`	Opcional	Cantidad de nodos de almacenamiento de Swift que se agregarán. Si no se introduce un valor, se utiliza `1` de forma predeterminada.
`--disk-size`	Opcional	Tamaño de disco en gigabytes para los nuevos nodos de almacenamiento de Swift. Si no se introduce un valor, se utiliza `2048` de forma predeterminada.
`-f` o `--json-file`	Opcional	Archivo JSON que contiene los parámetros para crear los nodos de almacenamiento.

El formato del archivo JSON es el siguiente:

```
{
        "storage_node_number": nodes,
        "storage_settings": [
                {
                        "datastore_name": "ds1",
                        "zone_number": ds1-zone,
```

```
                        "disk_size": ds1-disk-gb
                }
        ]
}
```

Cree una copia del contenido de la sección `storage_settings` para cada nodo de almacenamiento que desee crear.

Si no desea usar un archivo JSON para agregar nodos de almacenamiento, los números de zona se asignarán a los almacenes de datos especificados en orden. Puede usar el parámetro `zone_number` en el archivo JSON para asignar números de zona específicos o para colocar varios almacenes de datos en la misma zona. Un solo almacén de datos no puede ubicarse en varias zonas.

`viocli swift add-proxy [-d NAME] [--proxy-node-count PROXY-NODES] [-p] [--verbose]`

Agrega nodos de proxy a un clúster de Swift existente.

Parámetro	Obligatorio u opcional	Descripción
`--proxy-node-count`	Opcional	Cantidad de nodos de proxy de Swift que se agregarán. Si no se introduce un valor, se utiliza 1 de forma predeterminada.

`viocli swift list-datastore-zone-mapping [-d NAME] [-p] [--verbose]`

Muestra todos los almacenes de datos y las zonas en las que se encuentran.

Comando viocli upgrade

Use el comando `viocli upgrade` para actualizar entre versiones superiores de VMware Integrated OpenStack.

El comando `viocli upgrade` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`-p` o `--progress`	Opcional	Muestra el progreso de la operación actual.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli upgrade –h` o `viocli upgrade ––help` para mostrar los parámetros del comando. También puede utilizar la opción `––help` o `–h` en cualquier acción para mostrar los parámetros de la acción. Por ejemplo, `viocli upgrade prepare –h` muestra los parámetros para la acción `prepare`.

viocli upgrade mgmt_server [–d *NAME*] *DIR–NAME NFS–VOLUME* [–p] [––verbose]

Actualiza la configuración y la base de datos del servidor de administración a la versión deseada. Los siguientes parámetros adicionales se aplican a la acción `mgmt_server`.

Parámetro	Obligatorio u opcional	Descripción
DIR-NAME	Obligatorio	Directorio que contiene el archivo de copia de seguridad.
NFS-VOLUME	Obligatorio	Nombre o dirección IP del volumen NFS de destino y del directorio con el formato *remote-host*:*remote-dir*. Por ejemplo: `192.168.1.77:/backups`

viocli upgrade prepare [–d *NAME*] *BLUE–OMS–SERVER NFS–DIR–NAME* [*BLUE–VIOUSER–PASSWORD*] [–f] [–p] [––verbose]

Prepara el servidor NFS para la actualización de Servidor de administración de OpenStack. Los siguientes parámetros adicionales se aplican a la acción `prepare`.

Parámetro	Obligatorio u opcional	Descripción
BLUE-OMS-SERVER	Obligatorio	Dirección IP de la instancia anterior de Servidor de administración de OpenStack.
NFS-DIR-NAME	Obligatorio	Punto de montaje local para asociar el volumen NFS de destino.
BLUE-VIOUSER-PASSWORD	Opcional	Contraseña de la cuenta `viouser` en la instancia anterior de Servidor de administración de OpenStack. Si no incluye esta opción en el comando, se le solicitará que introduzca la contraseña.
`–f` o `––force`	Opcional	Ejecuta el comando sin solicitar una confirmación.

viocli upgrade openstack [–d *NAME*] [–n *NEW–DEPLOY*] [–f] [–p] [––verbose]

Actualiza la implementación de VMware Integrated OpenStack a la versión deseada.

Nota Si es posible, utilice vSphere Client para actualizar la implementación en lugar de este comando.

Los siguientes parámetros adicionales se aplican a la acción `openstack`.

Parámetro	Obligatorio u opcional	Descripción
`-n` *NEW-DEPLOY*	Opcional	Nombre de la implementación para la nueva versión. Si no incluye esta opción en el comando, se le solicitará que introduzca un nombre.
`-f` o `--force`	Opcional	Ejecuta el comando sin solicitar una confirmación.

Comando viocli volume-migrate

Use el comando `viocli volume-migrate` para migrar uno o varios volúmenes de Cinder no asociados de un almacén de datos a otro.

Nota Para migrar los volúmenes asociados, debe migrar toda la instancia.

Para migrar los volúmenes de máquinas virtuales de sombra, utilice el comando `viocli ds-migrate-prep` y, a continuación, complete la migración mediante vSphere Client.

El comando `viocli volume-migrate` usa la siguiente sintaxis.

```
viocli volume-migrate [-d NAME] {--volume-ids UUID1[,UUID2...] | --source-dc SRC-DC-NAME --source-ds SRC-DS-NAME] DEST-DC-NAME DEST-DS-NAME [--ignore-storage-policy] [--verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`--volume-ids` *UUID1*	Obligatorio a menos que se utilicen `--source-dc` y `--source-ds`	Migra uno o varios volúmenes especificados por UUID. Para especificar varios volúmenes, separe los UUID con comas. Por ejemplo, el siguiente comando migra dos volúmenes al almacén de datos DS-01 en el centro de datos DC-01. `viocli volume-migrate --volume-ids 25e121d9-1153-4d15-92f8-c92c10b4987f,4f1120e1-9ed4-421a-b65b-908ab1c6bc50 DC-01 DS-01`
`--source-dc` *SRC-DC-NAME*	Obligatorio a menos que se utilice `--volume-ids`	Identifica el centro de datos de origen. Esta opción debe utilizarse junto con la opción `--source-ds`.
`--source-ds` *SRC-DS-NAME*	Obligatorio a menos que se utilice `--volume-ids`	Identifica el almacén de datos de origen. Esta opción debe utilizarse junto con la opción `--source-dc`. Por ejemplo, el siguiente comando migra todos los volúmenes del almacén de datos DS-01 en el centro de datos DC-01 al almacén de datos DS-02 en el centro de datos DC-02. `viocli volume-migrate --source-dc DC-01 --source-ds DS-01 DC-02 DS-02`
DEST-DC-NAME	Obligatorio	Especifica el centro de datos de destino.
DEST-DS-NAME	Obligatorio	Especifica el almacén de datos de destino.

Parámetro	Obligatorio u opcional	Descripción
`--ignore-storage-policy`	Opcional	Ignora la comprobación de cumplimiento de la directiva de almacenamiento. Este parámetro permite la migración de volúmenes cuando el almacén de datos de destino no cumple con la directiva de almacenamiento del volumen migrado.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli volume-migrate -h` o `viocli volume-migrate --help` para mostrar los parámetros del comando.

Comando viocli vros

Use el comando `viocli vros` para permitir que VMware Integrated OpenStack interactúe con vRealize Automation.

El comando `viocli vros` usa la siguiente sintaxis.

```
viocli vros enable [-d NAME] -vt VRA-TENANT -vh VRA-HOST -va VRA-ADMIN -vrh VROS-HOST [--verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`-vt` *VRA-TENANT* o `--vra_tenant` *VRA-TENANT*	Obligatorio	Arrendatario al que pertenece el administrador del sistema vRealize Automation.
`-vh` *VRA-HOST* o `--vra_host` *VRA-HOST*	Obligatorio	IP o nombre del host de vRealize Automation.
`-va` *VRA-ADMIN* o `--vra_admin` *VRA-ADMIN*	Obligatorio	Nombre de usuario del administrador del sistema vRealize Automation.
`-vrh` *VROS-HOST* o `--vros_host` *VROS-HOST*	Obligatorio	IP o nombre del host del servicio de complemento de OpenStack para vRealize Orchestrator.
`--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli vros -h` o `viocli vros --help` para mostrar los parámetros del comando.

Comando viopatch add

Utilice el comando `viopatch add` para agregar nuevas revisiones a la implementación y poder instalarlas.

El comando `viopatch add` usa la siguiente sintaxis.

```
viopatch add -l PATCH-LOCATION
```

Parámetro	Obligatorio u opcional	Descripción
`-l` *PATCH-LOCATION* o `--location` *PATCH-LOCATION*	Obligatorio	Ruta de acceso del archivo de revisión que se agregará.

También puede ejecutar `viopatch add -h` o `viopatch add --help` para mostrar los parámetros del comando.

Comando viopatch install

Utilice el comando `viopatch install` para instalar revisiones de VMware Integrated OpenStack.

Debe usar el comando `viopatch add` para agregar revisiones antes de poder instalarlas.

El comando `viopatch install` usa la siguiente sintaxis.

```
viopatch install [-d NAME] -p PATCH-NAME -v PATCH-VERSION
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *NAME* o `--deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`-p` *PATCH-NAME* o `--patch` *PATCH-NAME*	Obligatorio	Nombre de la revisión que se instalará.
`-v` *PATCH-VERSION* o `--version` *PATCH-VERSION*	Obligatorio	Versión de la revisión que se instalará.

También puede ejecutar `viopatch install -h` o `viopatch install --help` para mostrar los parámetros del comando.

Comando viopatch list

Utilice el comando `viopatch list` para mostrar todas las revisiones de VMware Integrated OpenStack que se agregaron.

También puede ejecutar `viopatch list -h` o `viopatch list --help` para mostrar los parámetros del comando.

Comando viopatch snapshot

Utilice el comando `viopatch snapshot` para crear y administrar instantáneas de la implementación de OpenStack a fin de realizar una copia de seguridad previa a la revisión.

Importante El comando `viopatch snapshot take` detiene los servicios de OpenStack. Los servicios se iniciarán de nuevo cuando se instale la revisión. Si decide no instalar una revisión después de crear una instantánea, puede iniciar manualmente los servicios de OpenStack ejecutando el comando `viocli services start`.

El comando `viopatch snapshot` usa la siguiente sintaxis.

```
viopatch snapshot {take | revert | remove | list} [–d NAME] [–p] [––verbose]
```

Parámetro	Obligatorio u opcional	Descripción
`–d` *NAME* o `––deployment` *NAME*	Opcional	Nombre de la implementación que desea utilizar. Si no introduce un valor, se utiliza la implementación predeterminada.
`–p` o `––progress`	Opcional	Muestra el progreso de la operación actual.
`––verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viopatch snapshot –h` o `viopatch snapshot ––help` para mostrar los parámetros del comando.

Comando viopatch uninstall

El comando `viopatch uninstall` ya no es compatible.

Para revertir una revisión reciente, consulte "Revertir una revisión de VMware Integrated OpenStack" en *Guía de instalación y configuración de VMware Integrated OpenStack*.

Comando viopatch version

Utilice el comando `viopatch version` para mostrar la versión actual de VMware Integrated OpenStack.

También puede ejecutar `viopatch version –h` o `viopatch version ––help` para mostrar los parámetros del comando.