Guía de administración de VMware Integrated OpenStack

Modificada el 8 de junio de 2020
VMware Integrated OpenStack 6.0

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

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

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

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

Contenido

VMware Integrated OpenStack Administration Guide

1

The *VMware Integrated OpenStack Administration Guide* shows you how to perform administrative tasks in VMware Integrated OpenStack, including how to create and manage projects, users, accounts, flavors, images, and networks.

Intended Audience

This guide is for cloud administrators who want to create and manage resources with an OpenStack deployment that is fully integrated with VMware vSphere®. To do so successfully, you should be familiar with the OpenStack components and functions.

Terminology

For definitions of terms as they are used in this document, see the Glosario de VMware and the Glosario de OpenStack.

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

Puede escalar horizontalmente los nodos, los servicios, los clústeres y los almacenes de datos en la implementación de VMware Integrated OpenStack para adaptarse a una carga más alta.

Add Controller Nodes to Your Deployment

You can scale out your deployment by adding more controller nodes.

Nota The number of controller nodes in a deployment cannot be reduced. Ensure that you have sufficient resources before initiating a scale-out operation. Do not delete controller nodes through vSphere.

Procedimiento

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. In **OpenStack Deployment**, click the name of your deployment and open the **Nodes** tab.
3. Click **Scale Out Controller Node**.
4. Enter the desired number of controller nodes and click **OK**.

Resultados

The new controller nodes are created. Once the nodes are displayed in the table and their status has changed to `Ready`, they can be used as part of your deployment.

Escalar servicios de OpenStack

Puede escalar o reducir horizontalmente de manera dinámica los servicios de OpenStack para adaptarse a una carga del sistema cambiante.

Nota VMware Integrated OpenStack no permite escalar ni reducir horizontalmente los siguientes servicios:

- Gnocchi
- Ingress
- MariaDB
- Memcached
- Proceso para Nova
- RabbitMQ

No intente escalar ni reducir horizontalmente estos servicios mediante la interfaz web, la interfaz de línea de comandos ni la API.

Procedimiento

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
3. En la pestaña **Servicios**, busque el componente de OpenStack deseado y seleccione **Acciones > Escalar horizontalmente**.

4 Para cada servicio del componente, introduzca la cantidad deseada de pods.

Nota La cantidad máxima de réplicas de cada servicio no puede ser superior a la cantidad de nodos de trabajo.

5 Haga clic en **Aceptar**.

Resultados

Los pods de servicio se crean o finalizan para alcanzar el número especificado.

Agregar clústeres de proceso a la implementación

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

Requisitos previos

Nota Si desea agregar clústeres de proceso de una instancia de vCenter Server independiente, debe implementar VMware Integrated OpenStack con redes de NSX-T Data Center. Otros modos de redes no admiten la inclusión de clústeres de proceso de instancias de vCenter Server independientes.

Si agregó recursos a su entorno de vSphere después de implementar OpenStack, actualice la instancia de vCenter Server antes de continuar.

1 Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.

2 En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.

3 En la pestaña **Configuración**, haga clic en **Credenciales de vCenter**.

4 En la columna **Recursos de VC** de la instancia de vCenter Server correspondiente, haga clic en **Actualizar**.

Procedimiento

1 Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.

2 En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.

3 En la pestaña **Proceso**, haga clic en **Agregar**.

4 En **Configurar procesos para Nova**, haga clic en **Agregar**.

5 En el menú desplegable **vCenter Server**, seleccione la instancia de vCenter Server que contiene el clúster de proceso que desea agregar.

(Solamente NSX-T Data Center) Si no se muestra la instancia de vCenter Server que desea, haga clic en el icono **Agregar** (signo más) e introduzca el nombre de host y las credenciales.

6 Introduzca una zona de disponibilidad para el nuevo clúster de proceso.

   Los clústeres de proceso ubicados en instancias de vCenter Server diferentes no pueden estar en la misma zona de disponibilidad.

7 En el menú desplegable **Nombre del clúster**, seleccione el clúster de proceso que desee.

8 Seleccione uno o varios almacenes de datos para que los consuma el clúster de proceso y haga clic en **Enviar**.

Resultados

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

Pasos siguientes

Para agregar almacenes de datos a un clúster de proceso o eliminarlos de este, seleccione el clúster deseado y haga clic en **Editar**.

Para eliminar clústeres de proceso de la implementación, seleccione el clúster correspondiente y haga clic en **Eliminar**. Asegúrese de que todas las instancias de OpenStack del clúster se hayan eliminado antes de quitar el clúster.

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.

Requisitos previos

Nota Si desea agregar clústeres de proceso de una instancia de vCenter Server independiente, debe implementar VMware Integrated OpenStack con redes de NSX-T Data Center. Otros modos de redes no admiten la inclusión de clústeres de proceso de instancias de vCenter Server independientes.

Si agregó recursos a su entorno de vSphere después de implementar OpenStack, actualice la instancia de vCenter Server antes de continuar.

1 Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.

2 En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.

3 En la pestaña **Configuración**, haga clic en **Credenciales de vCenter**.

4 En la columna **Recursos de VC** de la instancia de vCenter Server correspondiente, haga clic en **Actualizar**.

Procedimiento

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
3. Haga clic en la pestaña **Glance** y, a continuación, en **Agregar**.
4. En el menú desplegable **vCenter Server**, seleccione la instancia de vCenter Server que contiene el clúster de proceso que desea agregar.

   (Solamente NSX-T Data Center) Si no se muestra la instancia de vCenter Server que desea, haga clic en el icono **Agregar** (signo más) e introduzca el nombre de host y las credenciales.
5. Seleccione uno o varios almacenes de datos que desee agregar y haga clic en **Siguiente**.
6. Revise la configuración propuesta y haga clic en **Enviar**.

Resultados

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

Pasos siguientes

Puede seleccionar un almacén de datos y hacer clic en **Eliminar** para quitarlo del servicio de imágenes.

Agregar clústeres al servicio de almacenamiento en bloque

Puede agregar clústeres al servicio de almacenamiento en bloque para aumentar la capacidad de almacenamiento de los volúmenes.

Requisitos previos

Nota Si desea agregar clústeres de proceso de una instancia de vCenter Server independiente, debe implementar VMware Integrated OpenStack con redes de NSX-T Data Center. Otros modos de redes no admiten la inclusión de clústeres de proceso de instancias de vCenter Server independientes.

Si agregó recursos a su entorno de vSphere después de implementar OpenStack, actualice la instancia de vCenter Server antes de continuar.

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
3. En la pestaña **Configuración**, haga clic en **Credenciales de vCenter**.
4. En la columna **Recursos de VC** de la instancia de vCenter Server correspondiente, haga clic en **Actualizar**.

Procedimiento

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
3. En la pestaña **Cinder**, haga clic en **Agregar**.
4. En el menú desplegable **vCenter Server**, seleccione la instancia de vCenter Server que contiene el clúster de proceso que desea agregar.

   (Solamente NSX-T Data Center) Si no se muestra la instancia de vCenter Server que desea, haga clic en el icono **Agregar** (signo más) e introduzca el nombre de host y las credenciales.
5. Seleccione **VMDK** o **FCD** como el controlador de back-end.
6. Introduzca una zona de disponibilidad para el nuevo clúster.
7. En la tabla, seleccione el clúster de proceso que desee.

Resultados

La capacidad del servicio de almacenamiento en bloque aumenta junto con el tamaño del clúster adicional.

Pasos siguientes

Para eliminar clústeres de la implementación, seleccione el clúster deseado y haga clic en **Eliminar**.

Habilitar HA en la implementación

Si implementó VMware Integrated OpenStack en el modo que no es de HA, puede convertir la implementación al modo de HA.

Nota Esta acción no se puede revertir. Las implementaciones de HA no se pueden convertir al modo que no es de HA.

Requisitos previos

Compruebe que el entorno contenga suficientes recursos para implementar los nodos adicionales que requiere el modo de HA. Consulte Requisitos de hardware de VMware Integrated OpenStack.

Procedimiento

1. Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

   ```
   ssh root@mgmt-server-ip
   ```

2 Habilite el modo de HA en la implementación.

```
viocli update deployment --enable-ha
```

Resultados

Se crean nodos de controladora adicionales y se actualizan las configuraciones de servicio para habilitar HA en la implementación.

Modificar redes de administración y de acceso a la API

Si implementó la red de administración y la red de acceso a la API sin DHCP, puede agregar rangos de direcciones IP y cambiar los servidores DNS después de la implementación.

Las redes que utilizan DHCP no se pueden modificar.

Procedimiento

1 Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.

2 En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.

3 En la pestaña **Red**, seleccione la red que desea modificar.

- Para agregar un rango de direcciones IP, seleccione **Agregar rango de IP** e introduzca el rango de direcciones IP que desea agregar a la red.

  En el cuadro de diálogo que se muestra, puede hacer clic en **Agregar rango de IP** para agregar varios rangos de direcciones IP a la vez.

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

- Para cambiar el servidor DNS, seleccione **Cambiar DNS** e introduzca los servidores DNS que desea agregar a la red.

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

Update Component Credentials

You can modify the credentials with which your VMware Integrated OpenStack deployment accesses and connects with your NSX Manager and vCenter Server instance.

Procedimiento

1 Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.

2 En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.

3 On the **Settings** tab, update the desired credentials.

- To update the credentials for a vCenter Server instance, select **vCenter Credentials**. You can click **Add** to add an instance to your deployment, or select an existing instance and click **Edit** or **Delete**.
- To update the credentials for NSX-T Data Center, select **NSX-T Credentials**, select your credentials, and click **Edit**.

4 Enter the desired credentials and click **OK**.

Agregar certificados a la implementación

Puede actualizar los certificados digitales de los servicios de OpenStack en la implementación.

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 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Ejecute el comando `viocli create csr` para generar solicitudes de firma del certificado para los servicios deseados.

```
viocli create csr [-c country-name] [-t state-name] [-l city-name] [-n org-name] [-u org-unit] [-
s service1,...] [-d output-directory]
```

Para ver la sintaxis del comando, consulte Comando viocli create.

3 Use las CSR generadas para obtener certificados de una CA.

4 Transfiera los certificados a un directorio de Integrated OpenStack Manager.

5 Ejecute el comando `viocli import certificate` para importar los certificados en VMware Integrated OpenStack.

```
viocli import certificate -d cert-directory
```

6 Reinicie los servicios de OpenStack para que surtan efecto los nuevos certificados.

```
viocli stop services
viocli start services
```

Resultados

Los nuevos certificados se importan en la implementación. Puede ejecutar el comando `viocli get certificates` para ver el certificado actual de cada servicio.

Profile OpenStack Services

You can use OSProfiler to enable tracing for the core services in your OpenStack deployment. Tracing captures the response time of all API, RPC, driver, and database calls that are part of an OpenStack operation.

VMware Integrated OpenStack supports the profiling of Cinder, Glance, Heat, Neutron, Nova, and Keystone commands. Profiler trace data is stored in vRealize Log Insight.

Requisitos previos

Deploy and configure vRealize Log Insight. See the Introducción document for vRealize Log Insight.

Procedimiento

1. Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

   ```
   ssh root@mgmt-server-ip
   ```

2. Modify the configuration of the service that you want to profile.

   ```
   viocli update service-name
   ```

3. Create the `profiler` section.
4. Add the `enabled` parameter and set its value to **`true`**.
5. If you want to trace database calls, add the `trace_sqlalchemy` parameter and set its value to **`true`**.
6. Add the `hmac_keys` parameter and enter a password for OSProfiler.
7. Add the `connection_string` parameter and set its value to the location of your vRealize Log Insight server.

   Enter the vRealize Log Insight server address in the following format: `loginsight://` *`username`*`:`*`password`*`@`*`loginsight-ip`*

   Specify the user name and password of a user with the `USER` role on your vRealize Log Insight deployment. Use percent encoding for any special characters in the user name or password. For example, replace a colon (:) with `%3A` and an at sign (@) with `%40`.

   The configuration file now looks similar to the following.

   ```
   conf:
     [...]
   profiler:
     enabled: true
     trace_sqlalchemy: true
     hmac_keys: osprofiler-password
     connection_string: loginsight://username:password@loginsight-ip
   ```

Resultados

You can now enable profiling on OpenStack commands. Run the desired command with the `--profile` parameter and specify your OSProfiler password. The command outputs a profiling trace UUID. Then generate a report by running OSProfiler with the profiling trace UUID and the vRealize Log Insight address. The following example profiles the `openstack volume list` command:

```
openstack --profile osprofiler-password volume list
osprofiler trace show --connection-string "loginsight://username:password@loginsight-ip" --html
profiling-uuid
```

Crear varias regiones de Horizon

Puede agregar endpoints de Keystone a la implementación con el fin de crear varias regiones de Horizon.

Procedimiento

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
3. En la pestaña **Región de Horizon**, haga clic en **Agregar**.
4. Introduzca el nombre de la región y el endpoint de Keystone correspondiente (por ejemplo, https://192.0.2.45:5000/v3).
5. Haga clic en **Aceptar**.

Resultados

Se crea la nueva región y se muestra en la tabla. Tenga en cuenta que la región predeterminada de Horizon no se muestra y no se puede modificar.

Ahora, los usuarios pueden seleccionar la región deseada al iniciar sesión en Horizon.

Crear un tema personalizado para el panel de control de VMware Integrated OpenStack

Puede modificar el icono de marcador, el estilo y los logotipos del tema de VMware en el panel de control de VMware Integrated OpenStack.

El tema personalizado puede incluir los siguientes elementos:

- `_styles.scss`: estilos adicionales
- `_variables.scss`: definiciones de códigos de color
- `favicon.ico`: icono de marcador del panel de control de VMware Integrated OpenStack

- `logo.svg`: gráfico que se muestra en la esquina superior izquierda de cada página
- `logo-splash.svg`: gráfico que se muestra en la página de inicio de sesión

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.

Procedimiento

1. Cree un directorio llamado `temas` que incluya los archivos de temas personalizados.

   Utilice la siguiente estructura de directorio:

   - Los archivos `_styles.scss` y `_variables.scss` deben estar en el directorio `temas`.
   - Los archivos `favicon.ico`, `logo.svg` y `logo-splash.svg` deben estar en el directorio `temas/img`.

   No es necesario incluir los cinco archivos en el tema. Por ejemplo, puede optar por incluir solo logotipos personalizados y utilizar los estilos predeterminados.
2. Archive el directorio `themes` en un archivo TAR llamado `themes.tar`.

   Nota El nombre de archivo TAR debe ser `themes.tar`.
3. En vSphere, cree una biblioteca de contenido y cargue el archivo `themes.tar` en ella.

   Para obtener información sobre bibliotecas de contenido, consulte Usar bibliotecas de contenido.
4. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
5. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
6. En la pestaña **Configuración**, seleccione **Tema de Horizon** y haga clic en **Habilitar**.
7. Introduzca el nombre de la biblioteca de contenido que contiene el archivo `temas.tar` y haga clic en **Aceptar**.

Resultados

El servicio del panel de control de VMware Integrated OpenStack se reinicia y carga los archivos de temas personalizados. Una vez que el servicio esté disponible, puede iniciar sesión y cambiar al tema de VMware para mostrar las personalizaciones.

Pasos siguientes

En la página **Tema de Horizon**, puede hacer clic en **Editar** para especificar otra biblioteca de contenido o en **Deshabilitar** para dejar de utilizar el tema personalizado.

Nota Después de editar o deshabilitar el tema personalizado, borre la memoria caché del explorador para que se pueda mostrar el tema actualizado.

Personalizar la configuración de OpenStack

Use el comando `viocli update` a fin de establecer valores personalizados para los parámetros de OpenStack.

En las versiones anteriores de VMware Integrated OpenStack, se utilizaba el archivo personalizado `custom.yml` para modificar los parámetros de OpenStack. Esta implementación se reemplazó con el comando `viocli update`. Para obtener más información, consulte Comando viocli update.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Modifique la configuración de un servicio.

```
viocli update service-name
```

La configuración de servicio especificada se abre en un editor de texto.

3 Realice los cambios que desee, guarde el archivo y salga del editor de texto.

Resultados

La implementación de OpenStack se actualiza y refleja la configuración que modificó.

Cambia el nombre de un almacén de datos

Puede usar el comando `viocli update` para cambiar el nombre de un almacén de datos. La especificación del almacén de datos varía según el tipo de servicio.

Para modificar parámetros de OpenStack, utilice el comando `viocli update`. Para obtener más información, consulte Comando viocli update.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Enumere los recursos de cada tipo de servicio.
   - Para Cinder, escriba: `viocli get cinder`.
   - Para Glance, escriba: `viocli get glance`.
   - Para nova-compute, escriba: `viocli get novacompute`.
3 Especifique el recurso que desea actualizar. Si un tipo de servicio tiene varios recursos, incluya el nombre del recurso que se va a actualizar como en el ejemplo de nova-compute.
   - Para Cinder, escriba: `viocli update cinder`.
   - Para Glance, escriba: `viocli update glance`.
   - Para nova-compute, escriba: `viocli update novacompute <name_of_resource>`.

   La configuración de servicio especificada se abre en un editor de texto.
4 Cambie el nombre o la expresión regular por un valor que coincida con el nombre del almacén de datos.
   - Para Cinder, cambie el valor del parámetro `vmware_datastore_regex`.
   - Para Glance, cambie el valor del parámetro `vmware_datastores`.
   - Para nova-compute, cambie los valores de los parámetros `datastore_regex` y `shared_datastore_regex`.
5 Guarde el archivo y salga del editor de texto.

Resultados

Ha cambiado el nombre de un almacén de datos en la implementación 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.

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 calidad de servicio para instancias.

Puede administrar centros de datos virtuales de tenant mediante la utilidad `viocli`, 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.

Requisitos previos

- Habilite las funciones de VMware Integrated OpenStack Carrier Edition. Consulte Habilitar funciones de Carrier Edition.
- Determine el UUID del proyecto en el que desea crear el VDC de tenant. Para encontrar UUID de proyecto, ejecute el comando `openstack project list`.
- Determine el nombre del nodo informático en el que desea crear el VDC de tenant. Para poder encontrar los nombres de los nodos informáticos, ejecute el comando `openstack compute service list`.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Cree un centro de datos virtual de tenant.

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

Opción	Descripción
--compute *compute-node*	Introduzca el nodo informático en el que se creará el VDC de tenant. Para poder encontrar los nombres de los nodos informáticos, ejecute el comando `openstack compute service list`.
--name *vdc-name*	Introduzca el nombre del VDC de tenant.
--project-id *project-uuid*	Introduzca el UUID del proyecto en el cual se va a crear el VDC de tenant.
--cpu-reserve *cpu-min*	Introduzca los ciclos de CPU en MHz que se reservarán para el VDC. Si no se incluye este parámetro, se utiliza `0` de forma predeterminada.
--cpu-limit *cpu-max*	Introduzca el límite máximo para el uso de CPU en el VDC (en MHz). Si no incluye este parámetro, el uso de CPU no es limitado.

Opción	Descripción
`--mem-reserve` *memory-min*	Introduzca la memoria en megabytes que se reservará para el VDC. Si no se incluye este parámetro, se utiliza `0` de forma predeterminada.
`--mem-limit` *memory-max*	Introduzca el límite máximo para el uso de memoria en el VDC (en megabytes). Si no incluye este parámetro, el uso de memoria no es limitado.

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 utilizar el centro de datos virtual de tenant.

   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 get tenant-vdcs` en Integrated OpenStack Manager para buscar el UUID de todos los centros de datos virtuales de tenant.

Resultados

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 get tenant-vdcs` *`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 un centro de datos virtual de tenant mediante la ejecución del comando `viocli update tenant-vdc` o eliminar un centro de datos virtual de tenant mediante el comando `viocli delete tenant-vdc`.

Usar las vAPI del centro de datos virtual de tenant

VMware Integrated OpenStack incluye una vAPI que puede utilizar para administrar 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`.

Cuando use la 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]
```

Eliminar una implementación de OpenStack

Si la implementación no se realizó correctamente o debe reconfigurarse, puede eliminar la implementación y volver a crearla.

Requisitos previos

Compruebe que se haya tomado una instantánea de Integrated OpenStack Manager antes de crearse la implementación actual. Si no tiene una instantánea de Integrated OpenStack Manager, debe eliminar el dispositivo virtual de VMware Integrated OpenStack y volver a instalarlo.

Procedimiento

1. En vSphere Client, apague las máquinas virtuales de la controladora y el dispositivo virtual de VMware Integrated OpenStack.
2. Elimine todas las máquinas virtuales de la controladora de VMware Integrated OpenStack presentes en el grupo de recursos.

   No elimine la plantilla de controladora en el dispositivo virtual de VMware Integrated OpenStack.
3. Restaure la máquina virtual de Integrated OpenStack Manager a la instantánea tomada antes de la implementación.
4. Encienda el dispositivo virtual de VMware Integrated OpenStack.

Resultados

Ahora puede crear una nueva implementación en Integrated OpenStack Manager. Consulte Crear una implementación de OpenStack.

Configuración de red de Neutron 3

Con Neutron, puede crear redes, configurar zonas de disponibilidad y realizar otras tareas de red avanzadas para la implementación de OpenStack.

Para obtener más información sobre Neutron, consulte la Documentación de OpenStack Neutron.

Este capítulo incluye los siguientes temas:

- Crear una red del proveedor
- Crear una red externa
- Crear una red de tenant
- Crear un puente de capa 2
- Crear una zona de disponibilidad de Neutron con NSX-T Data Center
- Configurar VMware Integrated OpenStack con un clúster de NSX Manager
- Usar el modo de ruta de acceso de datos mejorada de N-VDS para NSX-T Data Center con OpenStack
- Configurar la transparencia de VLAN
- Configurar el aprendizaje de direcciones MAC
- Especificar los tipos de enrutador de tenant para NSX Data Center for vSphere
- Agregar un back-end de NSX-T Data Center a una implementación de NSX Data Center for vSphere
- Crear un grupo de seguridad del proveedor
- Usar directivas de seguridad de NSX Data Center for vSphere en OpenStack
- Crear un equilibrador de carga
- Crear una zona de DNS

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.
- Para utilizar DHCP con nodos de NSX Edge con factor de forma de máquina virtual, habilite la transmisión manipulada y el modo promiscuo en el grupo de puertos que contiene los nodos de Edge. Para obtener instrucciones, consulte Configurar la directiva de seguridad para un grupo de puertos distribuido o un puerto distribuido.

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.
- Para utilizar DHCP en una red basada en VLAN con nodos de NSX Edge con factor de forma de máquina virtual, debe habilitar la transmisión manipulada y el modo promiscuo en el grupo de puertos que contiene los nodos de Edge. Para obtener instrucciones, consulte Configurar la directiva de seguridad para un grupo de puertos distribuido o un puerto distribuido.
- 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).
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).

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 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 de tenant

Puede crear redes lógicas de tenants en el panel de control de VMware Integrated OpenStack.

Nota VMware Integrated OpenStack no admite una red de tenants con redes VDS.

Procedimiento

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

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

3 Seleccione **Proyecto > Red > Redes**.

4 Haga clic en **Crear red** e introduzca la configuración deseada.

Opción	Descripción
Nombre de la red	Introduzca un nombre para la red de tenant.
Habilitar estado de administración	Active la casilla de verificación para habilitar la red. La red no se puede usar mientras el estado de administrador no esté activo.
Compartida	Seleccione la casilla de verificación para permitir que varios proyectos usen la red.

Opción	Descripción
Crear subred	Seleccione la casilla de verificación para utilizar este asistente para crear una subred en la red.
Sugerencias de zona de disponibilidad	Seleccione una zona de disponibilidad para crear la red en esa zona.

5 Si seleccionó **Crear subred**, haga clic en **Siguiente** e introduzca la configuración de subred deseada.

Opción	Descripción
Nombre de la subred	Introduzca un nombre para la subred.
Dirección de red	Introduzca la dirección de red de 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 la puerta de enlace de red. Si no introduce ningún valor, se utilizará la primera dirección IP de la subred. Si no desea una puerta de enlace en la red, seleccione **Deshabilitar puerta de enlace**.

6 Haga clic en **Siguiente** y especifique atributos adicionales para la subred.

Opción	Descripción
Habilitar DHCP	Seleccione la casilla de verificación para habilitar DHCP en la red.
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 cada grupo en una línea independiente como dos direcciones IP separadas por una 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.
Servidores DNS	Introduzca las direcciones IP de los servidores DNS que se utilizarán en la subred. Introduzca cada dirección IP en una línea independiente.
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`**).

7 Haga clic en **Crear**.

Resultados

La red se crea y se muestra en la siguiente tabla.

Pasos siguientes

En la columna **Acciones de**, puede agregar más subredes a la red, editar su configuración o eliminarla.

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.

Nota El complemento de NSX-T Policy no es compatible con el puente de capa 2.

Requisitos previos

En NSX-T Data Center, cree un perfil de puente perimetral. Consulte Crear un perfil de puente de Edge en la *Guía de administración de NSX-T*.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Abra el cuadro de herramientas y establezca la contraseña de la cuenta de `admin`.

```
toolbox
export OS_PASSWORD=admin-account-password
```

3 Cree una puerta de enlace lógica de capa 2,

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

Para el valor de *edge-cluster-uuid*, introduzca el UUID del clúster de NSX Edge para el que configuró el perfil de puente perimetral.

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

4 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
```

Resultados

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 Data Center for vSphere 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 Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Abra el cuadro de herramientas y establezca la contraseña de la cuenta de `admin`.

```
toolbox
export OS_PASSWORD=admin-account-password
```

3 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*".

4 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
```

Resultados

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

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 cómo crear 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 Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Modifique la configuración de Neutron.

```
viocli update neutron
```

3 En la sección `nsx`, cree una sección para la nueva zona de disponibilidad.

Use el formato `az:`*`zone-name`*`:` para el nombre de la sección.

4 En la sección correspondiente a la nueva zona de disponibilidad, agregue el parámetro `dhcp_profile` y establezca su valor como el nombre del perfil de DHCP que se configuró para la zona de disponibilidad.

5 Agregue el parámetro `metadata_proxy` y establezca su valor como el nombre del servidor proxy de metadatos que se configuró para la zona de disponibilidad.

6 Si desea utilizar zonas de transporte independientes, agregue los parámetros `default_overlay_tz` y `default_vlan_tz`, y establezca sus valores como los nombres de la zona de transporte superpuesta y la de VLAN para la zona de disponibilidad.

7 En la sección `nsx_v3`, agregue el parámetro `availability_zones` y establezca su valor como los nombres de las zonas de disponibilidad separados por comas (,).

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  metadata_agent:
    [...]
  plugins:
    nsx:
      az:zone1-name:
        dhcp_profile: dhcp1-uuid
        metadata_proxy: mdp1-uuid
      az:zone2-name:
        dhcp_profile: dhcp2-uuid
        metadata_proxy: mdp2-uuid
      nsx_v3:
        availability_zones: zone1-name, zone2-name
        [...]
manifests:
  [...]
pod:
  [...]
```

Resultados

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.

   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 Integrated OpenStack Manager como el usuario de `root`.

5 Modifique la configuración de Neutron.

```
viocli update neutron
```

6 Agregue la siguiente información:

```
conf:
  plugins:
    nsx:
      az:std-az:
        default_overlay_tz: std-overlay-tz
        default_vlan_tz: std-vlan-tz
        dhcp_profile: std-dhcp
        metadata_proxy: std-mdp
      az:nfv-az:
        default_overlay_tz: nfv-overlay-tz
        default_vlan_tz nfv-vlan-tz
        dhcp_profile: nfv-dhcp
        metadata_proxy: nfv-mdp
      nsx_v3:
        availability_zones: std-az, nfv-az
```

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
```

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.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Modifique la configuración de Neutron para la implementación.

```
viocli update neutron
```

3 En la sección `nsx`, establezca el valor del parámetro `nsx_api_managers` en las direcciones IP de cada nodo del clúster de NSX Manager, con separación por comas.

```
nsx_api_managers: parent-manager-ip,manager-node2-ip,manager-node3-ip
```

Pasos siguientes

Si cambia la dirección IP de cualquier nodo, o si agrega o elimina nodos del clúster de NSX Manager, debe modificar la configuración de Neutron para incluir la información de dirección IP que se actualizó.

Usar el modo de ruta de acceso de datos mejorada de N-VDS para NSX-T Data Center con OpenStack

Para las implementaciones de NSX-T Data Center, puede crear redes y puertos respaldados por una zona de transporte a través del modo de ruta de acceso de datos mejorada de N-VDS.

Importante Esta función solo está disponible en VMware Integrated OpenStack Carrier Edition. Para obtener más información, consulte Licencias de VMware Integrated OpenStack.

Un conmutador virtual distribuido administrado por NSX (NSX-Managed Virtual Distributed Switch, N-VDS) puede funcionar en el modo de ruta de acceso de datos mejorada para proporcionar las mejoras de rendimiento de red necesarias para los flujos de trabajo de NFV. Para obtener más información, consulte Ruta de acceso a datos mejorada en la *Guía de instalación de NSX-T Data Center*.

Nota Si utiliza NSX-T Data Center 2.3.1, la seguridad de puertos no es compatible con el modo de ruta de acceso de datos mejorada de N-VDS. Debe deshabilitar la seguridad de puertos globalmente o para cada red de Neutron creada. Esta limitación está resuelta en NSX-T Data Center 2.4.

Requisitos previos

Si utiliza los modos de ruta de acceso de datos estándar y mejorada, cree una zona de disponibilidad independiente para el modo de ruta de acceso de datos mejorada. Consulte Crear una zona de disponibilidad de Neutron con NSX-T Data Center.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Modifique la configuración de Neutron.

```
viocli update neutron
```

3 En la sección `nsx_v3`, establezca el valor del parámetro `ens_support` en `true`.

4 Si utiliza NSX-T Data Center 2.3.1, agregue el parámetro `disable_port_security_for_ens` y establezca su valor en `true`.

Si lo prefiere, puede incluir el parámetro `--port-security-enabled=false` al crear una red de Neutron.

Pasos siguientes

Al crear redes que usan la ruta de acceso de datos mejorada de N-VDS, especifique la zona de disponibilidad creada para ella.

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 implementaciones 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 al crear la red. Por ejemplo:

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

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 Información sobre el perfil de conmutación de gestión de direcciones 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 Integrated OpenStack Manager como el usuario `root` y abra el cuadro de herramientas.

```
ssh root@mgmt-server-ip
toolbox
```

2 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
```

3 Habilite el aprendizaje de direcciones MAC en el puerto.

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

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 Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Modifique la configuración de Neutron.

```
viocli update neutron
```

3 En la sección `nsxv`, agregue el parámetro `tenant_router_types` y especifique los tipos de enrutador que desea que estén disponibles para los tenants.

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

Los valores del parámetro `tenant_router_types` se utilizan en orden como los tipos de enrutador predeterminados.

Resultados

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.

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.

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 Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

3 Para agregar el back-end de NSX-T Data Center a la implementación, habilite TVD.

```
viocli add tvd -m manager-ip -u username -p password [--insecure {true | false}] [--overlay-tz
overlay-zone] [--vlan-tz vlan-zone] [--tier-0-router t0-router] [--dhcp-profile dhcp-profile] [--
md-proxy mdp-server] [--md-proxy-secret mdp-secret]
```

Opción	Descripción
manager-ip	Introduzca la dirección IP de la instancia de NSX Manager de la implementación de NSX-T Data Center.
username	Introduzca el nombre de usuario del administrador de NSX Manager.
password	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`.
overlay-zone	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.
vlan-zone	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.
t0-router	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.
dhcp-profile	Introduzca el nombre o el UUID del perfil de servidor DHCP de NSX-T Data Center empleado para habilitar el servicio DHCP nativo.
mdp-server	Introduzca el nombre o el UUID del servidor proxy de metadatos de NSX-T Data Center usado para habilitar el servicio de metadatos nativo.
mdp-secret	Introduzca el secreto compartido del servidor proxy de metadatos de NSX-T Data Center.

4 Si desea seguir usando NSX Data Center for vSphere para determinados proyectos existentes, asigne inmediatamente esos proyectos al back-end de NSX Data Center for vSphere.

```
toolbox
openstack project plugin create project-uuid --plugin nsx-v
```

Resultados

La implementación está conectada a los back-ends de NSX Data Center for vSphere y NSX-T Data Center. De forma predeterminada, todos los proyectos utilizan el back-end de NSX-T Data Center, a menos que los asigne manualmente al back-end de NSX Data Center for vSphere.

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.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Abra el cuadro de herramientas y establezca la contraseña de la cuenta de `admin`.

```
toolbox
export OS_PASSWORD=admin-account-password
```

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

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

4 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.
--tenant-id	Introduzca el identificador del proyecto que contiene el grupo de seguridad del proveedor.
--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.
--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`.

Resultados

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*.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Modifique la configuración de Neutron.

```
viocli update neutron
```

3 En la sección `nsxv`, agregue los parámetros `use_nsx_policies`, `default_policy_id` y `allow_tenant_rules_with_policy`, y configúrelos.

Opción	Descripción
`use_nsx_policies`	Introduzca **`true`**.
`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, inicie sesión en vSphere Client y seleccione **Menú > Redes y seguridad**. Haga clic en **Service Composer** y abra la pestaña **Directivas de seguridad**. 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.
`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.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  [...]
  plugins:
    nsx:
      [...]
      nsxv:
        use_nsx_policies: true
        default_policy_id: policy-5
        allow_tenant_rules_with_policy: true
```

4 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, especifique la directiva deseada al crear el grupo:

```
toolbox
export OS_PASSWORD=admin-account-password
neutron security-group-create security-group-name --tenant-id tenant-uuid --policy=policy-id
```

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

```
kubectl -n openstack exec -it neutron-server-pod-name -- /bin/bash
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.

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

```
kubectl -n openstack exec -it neutron-server-pod-name -- /bin/bash
sudo -u neutron nsxadmin --config-file /etc/neutron/neutron.conf --config-file /etc/neutron/
plugins/vmware/nsx.ini -r firewall-sections -o nsx-reorder
```

Crear un equilibrador de carga

Puede crear equilibradores de carga para distribuir solicitudes entrantes entre instancias designadas. Los equilibradores de carga garantizan que las cargas de trabajo se compartan de forma predecible entre instancias y que los recursos del sistema se utilicen de forma más eficaz.

VMware Integrated OpenStack 6.0 es compatible con el equilibrador de carga como servicio (Load Balancer as a Service, LBaaS) con la versión 2.0 para implementaciones con redes de NSX Data Center for vSphere o NSX-T Data Center. El componente Octavia de OpenStack no es compatible con esta versión.

El proceso de configuración de LBaaS también crea un monitor de estado y lo asocia con el grupo de LBaaS. El monitor de estado es un servicio de Neutron que comprueba que las instancias sigan funcionando en el protocolo y el puerto especificados.

Nota No se admite el parámetro `admin_state` para los grupos de LBaaS en las implementaciones de NSX Data Center for vSphere y el establecimiento del estado de administrador de un grupo como inactivo no tiene ningún efecto. Para evitar que el tráfico de red llegue a los miembros de un grupo, establezca el estado de administrador de cada miembro como inactivo.

Los agentes de escucha de LBaaS pueden utilizar HTTP, TCP o HTTPS finalizado. Los agentes de escucha HTTPS finalizados finalizan TLS para las conexiones entrantes, y las claves y los certificados de TLS para estos agentes de escucha se almacenan en Barbican. Si desea crear agentes de escucha HTTPS finalizados, póngase en contacto con el administrador de nube para determinar si debe configurar ACL de manera que conceda al usuario `barbican` acceso a los secretos del proyecto.

Requisitos previos

- Cree un enrutador y una subred pública en la red. Para una implementación de NSX Data Center for vSphere, el tipo de enrutador debe ser `exclusive`.

  Nota Puede crear el equilibrador de carga en una subred de arrendatario, pero debe asignarle una dirección IP flotante.

- Configure al menos un cliente y al menos dos instancias de servidor.

Procedimiento

1. Si desea crear agentes de escucha HTTPS finalizados y necesita configurar ACL, conceda al usuario de `barbican` acceso a los certificados, las claves y los contenedores de TLS.
   a. Inicie sesión en Integrated OpenStack Manager como el usuario `root` y abra el cuadro de herramientas.

   ```
   ssh root@mgmt-server-ip
   toolbox
   ```

   b. Configure la ACL.

   ```
   openstack acl user add -u barbican-uuid object-name
   ```

   Ejecute este comando una vez para cada certificado, clave y contenedor en el proyecto.

   Puede ejecutar el comando `openstack user list` para encontrar el UUID del usuario de `barbican`. Puede ejecutar el comando `openstack secret list` para buscar los nombres de contenedor, certificado y clave.
2. Inicie sesión en el panel de control de VMware Integrated OpenStack.
3. En el menú desplegable de la barra de título, seleccione el proyecto.
4. Seleccione **Proyecto > Red > Equilibradores de carga Neutron** y haga clic en **Crear equilibrador de carga**.
5. En la página **Detalles del equilibrador de carga**, introduzca la configuración deseada y haga clic en **Siguiente**.

Opción	Descripción
Nombre	Introduzca un nombre para el equilibrador de carga.
Descripción	(Opcional) Introduzca una descripción del equilibrador de carga.
Dirección IP	(Opcional) Introduzca la dirección IP del equilibrador de carga.
Subred	Seleccione una subred para el equilibrador de carga. Solo los miembros de esta subred pueden agregarse al grupo de LBaaS.

6 En la página **Detalles del agente de escucha**, introduzca la configuración deseada y haga clic en **Siguiente**.

Opción	Descripción
Nombre	Introduzca un nombre para el agente de escucha.
Descripción	Introduzca una descripción del agente de escucha.
Protocolo	Seleccione el protocolo que usará el agente de escucha. Se admiten los siguientes protocolos: ■ HTTP ■ TCP ■ HTTPS finalizado ■ HTTPS Si selecciona HTTPS finalizado como el protocolo, también debe proporcionar el identificador del contenedor de TLS.
Puerto	Introduzca el puerto que usará el agente de escucha.

7 Si seleccionó el protocolo `TERMINATED_HTTPS`, especifique uno o varios certificados para el agente de escucha y haga clic en **Siguiente**.

8 Especifique el nombre, la descripción y el método de equilibrio de carga para el grupo de LBaaS y haga clic en **Siguiente**.

A continuación se describen los métodos de equilibrio de carga admitidos:

Método	Descripción
LEAST_CONNECTIONS	Las nuevas solicitudes del cliente se envían al servidor que tiene la menor cantidad de conexiones.
ROUND_ROBIN	Cada servidor se utiliza de forma alternada en función del peso que se le asignó.
SOURCE_IP	El mismo miembro del grupo gestiona todas las conexiones que proceden de la misma dirección IP de origen.

9 Seleccione las instancias de servidor y cliente para agregarlas al grupo de equilibradores de carga y haga clic en **Siguiente**.

10 Especifique los parámetros del monitor de estado y haga clic en **Siguiente**.

Parámetro	Descripción
Tipo de monitor	Especifique **HTTP**, **PING** o **TCP**.
Intervalo	Introduzca el tiempo en segundos entre el envío de sondas a los miembros.
Reintentos	Introduzca el número de errores de conexión permitidos antes de cambiar el estado del miembro a `INACTIVE`.
Tiempo de espera	Introduzca el tiempo en segundos que un monitor esperará por el establecimiento de una conexión antes de que se agote el tiempo de espera. El valor de tiempo de espera debe ser menor que el del intervalo.

Si selecciona **HTTP**, también debe configurar el método HTTP, el código de estado esperado y la dirección URL.

11 Haga clic en **Crear equilibrador de carga**.

12 Si creó el equilibrador de carga en una subred de arrendatario, asocie una dirección IP flotante al equilibrador de carga.

a Haga clic en la flecha abajo que se encuentra a la derecha del equilibrador de carga y seleccione **Asociar IP flotante**.

b Seleccione una dirección IP flotante o un grupo de estas, y haga clic en **Asociar**.

13 (opcional) Envíe solicitudes de prueba para validar la configuración de LBaaS.

a Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

b Cree una prueba en el archivo `index.html`.

c En el mismo directorio, inicie un servidor web.

```
sudo python -m SimpleHTTPServer 80
```

d Inicie sesión en la instancia del cliente.

e Ejecute el comando `wget` para comprobar que la carga de las solicitudes se está equilibrando correctamente en los servidores del grupo.

```
wget -O - http://mgmt-server-ip
```

Pasos siguientes

Puede abrir el equilibrador de carga y hacer clic en **Crear agente de escucha** para agregar agentes de escucha a este.

Crear una zona de DNS

Si OpenStack Designate (DNS como servicio) está configurado para el entorno, puede crear zonas de DNS y conjuntos de registros a pedido mediante el panel de control de VMware Integrated OpenStack.

Requisitos previos

Compruebe que el administrador de nube habilitó Designate para el entorno. Para obtener más información, consulte Habilitar el componente Designate.

Procedimiento

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

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

3 Seleccione **Proyecto > DNS > Zonas** y haga clic en **Crear zona**.

Si no aparece la opción **DNS**, significa que no se habilitó Designate.

4 Especifique los parámetros para la zona de DNS y haga clic en **Enviar**.

Opción	Descripción
Nombre	Introduzca la zona de DNS. El valor debe terminar con un punto (.).
Descripción	Introduzca detalles acerca de la zona.
Dirección de correo electrónico	Introduzca la dirección de correo electrónico del propietario de la zona.
TTL	Especifique el período de vida (Time To Live, TTL) en segundos de los registros de la zona.
Tipo	Seleccione si desea crear una zona principal o una secundaria.

5 Haga clic en **Crear conjunto de registros**.

6 Especifique los parámetros para el conjunto de registros y haga clic en **Enviar**.

Opción	Descripción
Tipo	Seleccione el tipo de conjunto de registros. Se admiten los siguientes valores: ■ A (registro de dirección) ■ AAAA (registro de dirección IPv6) ■ CNAME (registro de nombre canónico) ■ MX (registro Mail eXchange) ■ PTR (registro de puntero) ■ SPR (marco de directivas de remitente) ■ SRV (localizador de servicios) ■ SSHFP (huella digital de clave pública de SSH) ■ TXT (registro de texto)
Nombre	Introduzca el nombre de dominio para el conjunto de registros. El valor debe terminar con un punto (.).
Descripción	Introduzca detalles sobre el conjunto de registros.
TTL	Especifique el valor de TTL en segundos para los registros del conjunto de registros.
Registros	Especifique uno o varios registros para incluirlos en el conjunto de registros. Haga clic en **Agregar registro** para agregar varios registros.

Puede crear uno o varios conjuntos de registros para cada zona.

Pasos siguientes

Puede hacer clic en el nombre de la zona en la página **Zonas de DNS** para obtener información sobre ella. Haga clic en la flecha abajo situada junto a **Crear conjunto de registros** y seleccione **Actualizar** o **Eliminar** para modificar o quitar la zona. En la pestaña **Conjuntos de registros**, puede actualizar o eliminar los conjuntos de registros en la zona.

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.

Para obtener más información sobre Keystone, consulte la Documentación de OpenStack Keystone.

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:

- Crear un proyecto de OpenStack
- Crear un usuario de nube
- Crear un grupo de usuarios
- Administrar dominios de Keystone
- Actualizar la contraseña de administrador de Keystone
- Configurar autenticación LDAP
- Configurar la federación de VMware Identity Manager
- Configurar la federación de Keystone a Keystone
- Configurar la federación de SAML 2.0 genérica

Crear un proyecto de OpenStack

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

Nota El dominio de un proyecto no se puede especificar a través del panel de control de VMware Integrated OpenStack. Para crear un proyecto en un dominio especificado, utilice la interfaz de línea de comandos 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 > Proyectos**.
4. Haga clic en **Crear proyecto** e introduzca la configuración deseada.

Opción	Descripción
Nombre	Introduzca un nombre para el proyecto.
Descripción	Escriba una breve descripción del proyecto.
Habilitado	Seleccione la casilla de verificación para habilitar el proyecto.

5. (opcional) Abra la pestaña **Miembros del proyecto** y agregue usuarios al proyecto.
6. (opcional) Abra la pestaña **Grupos del proyecto** y agregue grupos de usuarios al proyecto.
7. Haga clic en **Crear proyecto**.

Resultados

Se crea el proyecto y se le asigna un UUID.

Nota El UUID 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.
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.

Administrar dominios de Keystone

Los dominios de Keystone son contenedores para proyectos y usuarios.

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

Todas las implementaciones de VMware Integrated OpenStack contienen los dominios `service` y `Default`. El dominio `service` contiene las cuentas que usan los servicios de OpenStack y el dominio `Default` contiene las cuentas que utilizan los usuarios de OpenStack, incluida la cuenta de `admin`.

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

En versiones anteriores de VMware Integrated OpenStack, si se configuraba la autenticación LDAP durante la instalación, el dominio `Default` contenía usuarios LDAP y el dominio `local` contenía cuentas de usuario y servicio de OpenStack. Si actualizó la implementación a partir de una versión anterior de VMware Integrated OpenStack, esta configuración se mantiene para compatibilidad con versiones anteriores. Sin embargo, los usuarios del servicio se mueven al dominio `service`.

Actualizar la contraseña de administrador de Keystone

El proceso para actualizar la contraseña de usuario administrador de Keystone requiere dos pasos.

Nota La actualización activa la canalización de Lifecycle Manager de OpenStack y actualiza cada gráfico de Helm. Es posible que la actualización interrumpa los servicios de OpenStack durante un breve periodo.

Requisitos previos

Compruebe que tiene una contraseña con codificación Base64.

Procedimiento

1 Cambie la contraseña del usuario administrador de Keystone.

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

   b Seleccione **Identidad > Usuarios**.

   c En la columna Acciones, seleccione **Cambiar contraseña**.

   También puede utilizar la CLI de OpenStack para cambiar la contraseña con el siguiente comando.

```
openstack user set ––password <password> admin
```

   O bien, para cambiar la contraseña por una solicitud en lugar de escribir la contraseña, utilice el siguiente comando.

```
openstack user set ––password–prompt admin
```

2 En el espacio de nombres de OpenStack, cambie la contraseña de administrador de Keystone.

   a Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt–server–ip
```

   b Edite `secret managedpasswords`.

```
osctl edit secret managedpasswords
```

c Actualice el valor de **data.admin_password**.

```
apiVersion: v1
data:
  admin_password: <new_password>
```

El valor de *new_password* debe tener codificación Base64.

d Compruebe el estado de la implementación.

```
viocli get deployment
```

El estado de la implementación aparece primero como `reconfigurando`. Cuando llega a `en ejecución`, se completa la actualización de la contraseña.

Configurar autenticación LDAP

Puede configurar la autenticación LDAP, agregar nuevos dominios o modificar la configuración de LDAP existente.

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

De forma predeterminada, VMware Integrated OpenStack se conecta con el servidor de LDAP mediante SSL en el puerto 636. Si esta configuración no es adecuada para el entorno, especifique el puerto y el protocolo correctos en **Configuración avanzada**.

Requisitos previos

- Póngase en contacto con el administrador de LDAP para obtener la configuración de LDAP correcta para su entorno.
- Si desea utilizar un nuevo dominio de Keystone para los usuarios de LDAP, cree el dominio en Keystone antes de continuar. Los dominios `default`, `local` y `service` no se pueden utilizar para LDAP.

Procedimiento

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
3. En la pestaña **Configuración**, haga clic en **Configurar orígenes de identidad**.
4. Haga clic en **Agregar** para configurar un nuevo origen de LDAP o en **Editar** 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 para el origen de LDAP. **Nota** ■ No utilice `default`, `local` ni `service` como el dominio de Keystone. ■ El dominio de Keystone no se puede cambiar después de que se haya agregado el origen de LDAP. ■ Debe especificar un dominio de Keystone existente. Cree el dominio deseado antes de configurar la autenticación LDAP.
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 del usuario de LDAP.
Controladores de dominio	(Opcional) Introduzca las direcciones IP de uno o varios controladores de dominio separadas por comas (,). Si no especifica ningún controlador 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.
Ámbito de la consulta	Seleccione **SUB_TREE** para consultar todos los objetos bajo el objeto base o **ONE_LEVEL** para consultar solo los elementos secundarios directos del objeto base.
DN de árbol de usuario	(Opcional) Introduzca la base de búsqueda para los usuarios (por ejemplo, **DC=ejemplo,DC=com**).
Filtro de usuario	(Opcional) Introduzca un filtro de búsqueda de LDAP para los usuarios. **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 filtros, consulte Sintaxis de los filtros de búsqueda en la documentación de Microsoft.
DN de árbol de grupo	(Opcional) Introduzca la base de búsqueda para los grupos. El sufijo LDAP se utiliza de forma predeterminada.

Opción	Descripción
Filtro de grupo	(Opcional) Introduzca un filtro de búsqueda de LDAP para los grupos.
Usuario administrador de LDAP	Introduzca un usuario de LDAP para que actúe como administrador del dominio. Si especifica un usuario administrador de LDAP, el proyecto de `admin` se creará en el dominio de Keystone correspondiente a LDAP, y a este usuario se le asignará la función `admin` en ese proyecto. A continuación, el usuario puede iniciar sesión en Horizon y realizar otras operaciones en el dominio de Keystone para LDAP. Si no se especifica un usuario administrador de LDAP, se debe usar la interfaz de línea de comandos de OpenStack a fin de agregar un proyecto al dominio de Keystone para LDAP y asignar la función `admin` a un usuario de LDAP en ese proyecto.

6 (opcional) Active la casilla **Configuración avanzada** para mostrar campos de configuración de LDAP adicionales.

Opción	Descripción
Cifrado	Seleccione **Ninguno**, **SSL**o **StartTLS**.
Nombre de 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. El valor predeterminado es `organizationalPerson`.
Atributo de identificador de usuario	(Opcional) Introduzca el atributo de LDAP asignado al identificador de usuario. Este valor no puede ser un atributo con varios valores. El valor predeterminado es `cn`.
Atributo de nombre de usuario	(Opcional) Introduzca el atributo de LDAP asignado al nombre de usuario. El valor predeterminado es `userPrincipalName`.
Atributo de correo de usuario	(Opcional) Introduzca el atributo de LDAP asignado al correo electrónico de usuario. El valor predeterminado es `mail`.
Atributo de contraseña de usuario	(Opcional) Introduzca el atributo de LDAP asignado a la contraseña. El valor predeterminado es `userPassword`.
Máscara de bits habilitada por el usuario	Introduzca la máscara de bits que determina el bit que indica que un usuario está habilitado. Este valor debe ser un número entero. Si no se utiliza ninguna máscara de bits, introduzca `0`. El valor predeterminado es `2`.
Atributo objectclass para grupo	(Opcional) Introduzca la clase de objeto de LDAP para grupos. El valor predeterminado es `group`.
Atributo de identificador de grupo	(Opcional) Introduzca el atributo de LDAP asignado al identificador de grupo. El valor predeterminado es `cn`.
Atributo de nombre de grupo	(Opcional) Introduzca el atributo de LDAP asignado al nombre de grupo. El valor predeterminado es `sAMAccountName`.
Atributo de miembro de grupo	(Opcional) Introduzca el atributo de LDAP asignado al nombre de miembro de grupo. El valor predeterminado es `member`.
Atributo de descripción de grupo	(Opcional) Introduzca el atributo de LDAP asignado a la descripción de grupo. El valor predeterminado es `description`.

7 Haga clic en **Aceptar**.

VMware Integrated OpenStack valida la configuración de LDAP especificada.

8 Una vez finalizada la validación, acepte el certificado de la columna **CERT**.

9 Haga clic en **Configurar**.

10 Si no especificó un usuario administrador de LDAP, configure un proyecto y un administrador para el dominio de Keystone correspondiente a LDAP.

a Inicie sesión en Integrated OpenStack Manager como el usuario `root` y abra el cuadro de herramientas.

```
ssh root@mgmt-server-ip
toolbox
```

b Cree un proyecto en el dominio de Keystone para LDAP.

```
openstack project create new-project --domain ldap-domain
```

c Agregue un usuario de LDAP al nuevo proyecto.

```
openstack user set ldap-username --domain ldap-domain --project new-project --project-domain
ldap-domain
```

d En el dominio de Keystone para LDAP, asigne la función `admin` al usuario de LDAP.

```
openstack role add admin --user ldap-username --user-domain ldap-domain --domain ldap-domain
```

e En el nuevo proyecto, asigne la función `admin` al usuario de LDAP.

```
openstack role add admin --user ldap-username --user-domain ldap-domain --project new-project
--project-domain ldap-domain
```

Resultados

La autenticación LDAP está configurada en la implementación de VMware Integrated OpenStack. Puede iniciar sesión en el panel de control de VMware Integrated OpenStack como el usuario administrador de LDAP que especificó durante la configuración.

Nota Si necesita modificar la configuración de LDAP, debe utilizar la interfaz web de Integrated OpenStack Manager. No se admite la modificación de la configuración de LDAP a través de la línea de comandos.

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. Para obtener más información, consulte la Documentación de VMware Identity Manager.
- Si desea utilizar el protocolo OIDC y la instancia de VMware Identity Manager está utilizando un certificado autofirmado, asegúrese de que la CA esté instalada como una CA de confianza en VMware Identity Manager. Para obtener instrucciones, consulte Instalar certificados raíz de confianza en el documento *Instalar y configurar VMware Identity Manager*.
- Asegúrese de que su instancia de VMware Identity Manager puede comunicarse con la red de administración de VMware Integrated OpenStack.
- El usuario `admin` de OpenStack y el usuario `admin` de VMware Identity Manager no pueden estar en el mismo dominio de Keystone. Si desea importar usuarios federados al dominio `default`, asegúrese de que el usuario `admin` de VMware Identity Manager no forme parte del grupo de VMware Identity Manager que emplea para la federación.

Procedimiento

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
3. En la pestaña **Federación de identidades**, haga clic en **Agregar**.
4. En el menú desplegable **Tipo de federación**, seleccione **VIDM**.
5. Introduzca los parámetros requeridos.

Opción	Descripción
Tipo de protocolo	Seleccione **SAML2** u **OIDC** como el protocolo de identidad.
Nombre	Escriba un nombre para el proveedor de identidad. **Nota** El nombre del proveedor de identidad no se puede cambiar después de que se haya agregado el proveedor de identidad.
Descripción	Introduzca una descripción del proveedor de identidad.

Opción	Descripción
Dirección de VIDM	Introduzca el FQDN de la instancia de VMware Identity Manager sin el protocolo (por ejemplo, vidm.ejemplo.com). **Nota** El FQDN debe ser único. No se puede agregar una instancia única de VMware Identity Manager a VMware Integrated OpenStack como dos proveedores de identidad independientes.
Nombre de usuario de VIDM	Introduzca el nombre de usuario de un administrador de VMware Identity Manager.
Contraseña de VIDM	Introduzca la contraseña del administrador especificado.
Certificados de validación de VIDM	Seleccione la casilla de verificación para validar certificados de VMware Identity Manager. **Importante** Si seleccionó el protocolo OIDC y su instancia de VMware Identity Manager está usando un certificado autofirmado, debe validar los certificados.

6 (opcional) Seleccione la casilla de verificación **Configuración avanzada** para configurar parámetros adicionales.

a En **Configuración avanzada común**, introduzca un dominio, un proyecto y un grupo de OpenStack en los que se importarán los usuarios federados.

Nota

- Si no introduce un dominio, un proyecto o un grupo, se utilizan los siguientes valores predeterminados:
  - Dominio: `federated_domain`
  - Proyecto: `federated_project`
  - Grupo: `federated_group`
- No introduzca `federated` como el nombre de dominio. Este nombre está reservado por Keystone.
- Si proporciona asignaciones personalizadas, debe introducir todos los dominios, los proyectos y los grupos de OpenStack que se incluyen en dichas asignaciones.

b En el campo **Asignación de atributos**, introduzca atributos adicionales en formato JSON o cargue un archivo JSON que contenga los atributos deseados.

c En **Configuración avanzada de VIDM**, introduzca un tenant y un grupo de VMware Identity Manager desde el que se importarán usuarios.

Si está usando una instancia de VMware Identity Manager en una implementación de vRealize Automation, introduzca **`vsphere.local`** como el tenant. Si utiliza una instancia de VMware Identity Manager independiente, no introduzca un tenant.

d En **Configuración avanzada de SAML2**, introduzca la dirección URL del archivo de metadatos de federación de la instancia de VMware Identity Manager.

e En el campo **Asignación de SAML2**, introduzca las asignaciones de SAML en formato JSON o cargue un archivo JSON que contenga las asignaciones deseadas.

f En **Configuración avanzada de OIDC**, introduzca la dirección URL del archivo de metadatos de federación de la instancia de VMware Identity Manager.

g En el campo **Asignación de OIDC**, introduzca las asignaciones de OIDC en formato JSON o cargue un archivo JSON que contenga las asignaciones deseadas.

h En el campo **Asignación asignada**, introduzca asignaciones de OAuth en formato JSON o cargue un archivo JSON que contenga las asignaciones deseadas.

7 Haga clic en **Aceptar**.

Resultados

VMware Integrated OpenStack se crea como una aplicación web en VMware Identity Manager y los usuarios y grupos federados se importan de VMware Identity Manager a 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.

A los usuarios federados se les asigna automáticamente la función de miembro. Si es necesario, puede usar la interfaz de línea de comandos de OpenStack para asignar privilegios de administrador de nube a usuarios federados.

Nota Al utilizar la federación de identidades, debe acceder al panel de control de VMware Integrated OpenStack a través del endpoint de OpenStack público. No utilice el endpoint de OpenStack privado ni una dirección IP de controlador para iniciar sesión como usuario federado.

Pasos siguientes

Si necesita eliminar un proveedor de identidad configurado, primero selecciónelo en la interfaz web de Integrated OpenStack Manager y haga clic en **Eliminar**. A continuación, inicie sesión en el panel de control de VMware Integrated OpenStack, seleccione **Identidad > Federación > Proveedores de identidad**, seleccione el proveedor deseado y haga clic en **Eliminar del registro los proveedores de identidad**.

Configurar la federación de Keystone a Keystone

La federación de Keystone a Keystone (Keystone to Keystone, K2K) permite que varias implementaciones de OpenStack compartan el mismo origen de identidad. Resulta útil para los sitios que abarcan varias regiones, donde un sitio se utiliza como el origen de identidad.

Una implementación de VMware Integrated OpenStack puede configurarse como un proveedor de identidad o un proveedor de servicio para la federación de Keystone a Keystone. Un proveedor de identidad proporciona servicios de autenticación de usuario a un proveedor de servicio.

Procedimiento

1 Configure una implementación de OpenStack como un proveedor de identidad de Keystone.

a Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.

b En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.

c En la pestaña **Federación de identidades**, haga clic en **Agregar**.

d En el menú desplegable **Tipo de federación**, seleccione **K2K**.

e Introduzca los parámetros requeridos.

Opción	Descripción
Nombre	Escriba un nombre para el proveedor de identidad.
Descripción	Introduzca una descripción del proveedor de identidad.
Tipo de proveedor de K2K	Selecciones **Keystone como proveedor de identidad**.
Dirección del proveedor de servicio de K2K	Introduzca el endpoint de OpenStack público de la implementación de OpenStack que actuará como el proveedor de servicio (por ejemplo, 198.51.100.100).
CERTIFICADO DE CA de proveedor de servicio de K2K	Introduzca el contenido del certificado `vio.pem` desde la implementación de OpenStack que actuará como el proveedor de servicio. Para poder visualizar el contenido del archivo `vio.pem`, ejecute el siguiente comando: `kubectl –n openstack get secrets certs –o jsonpath='{@.data.vio_certificate}' | base64 ––decode`

f Haga clic en **Aceptar**.

2 Configure la segunda implementación de OpenStack como un proveedor de servicio de Keystone.

a Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.

b En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.

c En la pestaña **Federación de identidades**, haga clic en **Agregar**.

d En el menú desplegable **Tipo de federación**, seleccione **K2K**.

e Introduzca los parámetros requeridos.

Opción	Descripción
Nombre	Introduzca el nombre del proveedor de identidad de destino. El valor de este campo debe ser el mismo en ambas implementaciones.
Descripción	Introduzca una descripción del proveedor de servicio.
Tipo de proveedor de K2K	Seleccione **Keystone como proveedor de servicios**.
Dirección del proveedor de identidad de K2K	Introduzca el endpoint de OpenStack público de la implementación de OpenStack que actúa como el proveedor de identidad (por ejemplo, 192.0.2.100).
Puerto del proveedor de identidad de K2K	Introduzca el número de puerto de Keystone de la implementación de OpenStack que actúa como el proveedor de identidad (por ejemplo, 5000).

f (opcional) Puede seleccionar **Configuración avanzada > Configuración avanzada común** e introducir un dominio, un proyecto y un grupo de OpenStack en el que se importarán usuarios federados.

Nota

- Si no introduce un dominio, un proyecto o un grupo, se utilizan los siguientes valores predeterminados:
  - Dominio: `federated_domain`
  - Proyecto: `federated_project`
  - Grupo: `federated_group`
- No introduzca `federated` como el nombre de dominio. Este nombre está reservado por Keystone.
- Si proporciona asignaciones personalizadas, debe introducir todos los dominios, los proyectos y los grupos de OpenStack que se incluyen en dichas asignaciones.

g Haga clic en **Aceptar**.

Resultados

Los usuarios y los grupos se federan de la implementación del proveedor de servicio a la implementación del proveedor de identidad. Al iniciar sesión en el panel de control de VMware Integrated OpenStack en la implementación del proveedor de identidad, puede seleccionar el proveedor de servicio en la parte superior derecha de la página. A continuación, puede realizar acciones en la implementación del proveedor de servicio.

Nota Al utilizar la federación de identidades, debe acceder al panel de control de VMware Integrated OpenStack a través del endpoint de OpenStack público. No utilice el endpoint de OpenStack privado ni una dirección IP de controlador para iniciar sesión como 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 y configure el proveedor de identidades. Determine la ubicación del archivo de metadatos y el valor del atributo `entityID` en ese archivo.
- Asegúrese de que la implementación de VMware Integrated OpenStack puede acceder al FQDN del proveedor de identidad.
- Cree un archivo de asignación en formato JSON. Para obtener más información, consulte Combinaciones de asignación en la documentación de OpenStack.
- En el archivo de asignación, no utilice `federated` como nombre de dominio. Este nombre está reservado por Keystone.
- Cree un archivo de asignación de atributos SAML en formato JSON. Utilice la estructura siguiente:

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

Procedimiento

1. Inicie sesión en la interfaz web Integrated OpenStack Manager como el usuario de `admin`.
2. En **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.
3. En la pestaña **Federación de identidades**, haga clic en **Agregar**.
4. En el menú desplegable **Tipo de federación**, seleccione **Instancia genérica de SAML2**.

5 Introduzca los parámetros requeridos.

Opción	Descripción
Nombre	Escriba un nombre para el proveedor de identidad.
Descripción	Introduzca una descripción del proveedor de identidad.
Asignación de atributos	Introduzca atributos de SAML adicionales en formato JSON o cargue un archivo JSON que contenga los atributos deseados.
Instancia genérica de SAML2 no segura	Anule la selección de la casilla de verificación para validar los certificados del proveedor de identidad.
Identificador de entidad de instancia genérica de SAML2	Introduzca el atributo `entityID` para el proveedor de identidad. Puede encontrar este valor en el archivo de metadatos de federación.
URL de metadatos de SAML2	Introduzca la dirección URL del archivo de metadatos de federación del proveedor de identidad.
Asignación de SAML2	Introduzca asignaciones de SAML en formato JSON o cargue un archivo JSON que contenga las asignaciones deseadas.

6 (opcional) Seleccione la casilla de verificación **Configuración avanzada** para configurar parámetros adicionales.

a En **Configuración avanzada común**, introduzca un dominio, un proyecto y un grupo de OpenStack en los que se importarán los usuarios federados.

Nota

- Si no introduce un dominio, un proyecto o un grupo, se utilizan los siguientes valores predeterminados:
  - Dominio: `federated_domain`
  - Proyecto: `federated_project`
  - Grupo: `federated_group`
- No introduzca `federated` como el nombre de dominio. Este nombre está reservado por Keystone.
- Si proporciona asignaciones personalizadas, debe introducir todos los dominios, los proyectos y los grupos de OpenStack que se incluyen en dichas asignaciones.

7 Haga clic en **Aceptar**.

Resultados

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.

Nota Al utilizar la federación de identidades, debe acceder al panel de control de VMware Integrated OpenStack a través del endpoint de OpenStack público. No utilice el endpoint de OpenStack privado ni una dirección IP de controlador para iniciar sesión como usuario federado.

Ejemplo: Integrar VMware Integrated OpenStack con 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 función del nombre principal de usuario (User Principal Name, UPN). 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`. El nombre del proveedor de identidad en VMware Integrated OpenStack se establecerá en `adfsvio`.

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/adfsvio/Shibboleth.sso/SAML2`** para la dirección URL del usuario de confianza y haga clic en **Siguiente**.
   i Introduzca **`https://192.0.2.160:5000/adfsvio`** para el identificador de confianza del usuario de confianza, 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 la interfaz web Integrated OpenStack Manager como el usuario de `admin`.

3 En la **Implementación de OpenStack**, haga clic en el nombre de la implementación y abra la pestaña **Administrar**.

4 En la pestaña **Federación de identidades**, haga clic en **Agregar**.

5 En el menú desplegable **Tipo de federación**, seleccione **Instancia genérica de SAML2**.

6 Introduzca la siguiente configuración.

Opción	Descripción
Nombre	`adfsvio`
Descripción	`Proveedor de identidad de AD FS`
Asignación de atributos	`[ { "name": "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn", "id": "upn" } ]`
Identificador de entidad de instancia genérica de SAML2	`http://adfs.example.com/adfs/services/trust`

Opción	Descripción
URL de metadatos de SAML2	`https://adfs.example.com/federationmetadata/2007-06/federationmetadata.xml`
Asignación de SAML2	`[ { "local": [ { "user": { "name": "{0}" }, "group": { "domain": { "name": "adfs-users" }, "name": "Federated Users" } } ], "remote": [ { "type": "upn" } ] } ]`

7 Seleccione la casilla de verificación **Configuración avanzada**.

8 Seleccione **Configuración avanzada común** e introduzca la siguiente configuración.

Opción	Descripción
Dominio	`adfs-users`
Proyecto	Deje el campo vacío.
Grupo	`Usuarios federados`

Después de verificar y actualizar 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.

Pasos siguientes

Si necesita eliminar un proveedor de identidad configurado, primero selecciónelo en la interfaz web de Integrated OpenStack Manager y haga clic en **Eliminar**. A continuación, inicie sesión en el panel de control de VMware Integrated OpenStack, seleccione **Identidad > Federación > Proveedores de identidad**, seleccione el proveedor deseado y haga clic en **Eliminar del registro los proveedores de identidad**.

Instancias de OpenStack

5

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:

Administrar tipos de OpenStack

En OpenStack, un tipo es una configuración preestablecida en la que se define la capacidad de proceso, memoria y almacenamiento de una instancia.

Todas las implementaciones de VMware Integrated OpenStack contienen los siguientes tipos predeterminados.

Nombre	vCPU	RAM (GB)	Disco raíz (GB)
`m1.tiny`	1	0,5	1
`m1.small`	1	2	20
`m1.medium`	2	4	40
`m1.large`	4	8	80
`m1.xlarge`	8	16	160

Importante No elimine los tipos predeterminados.

Puede crear y administrar tipos adicionales según sea necesario. Para administrar los tipos de su implementación, inicie sesión en el panel de control de VMware Integrated OpenStack como administrador de nube y seleccione **Administrador > Proceso > Tipos**.

Iniciar una instancia

Puede iniciar una instancia desde una imagen, un volumen, una instantánea de instancia o una instantánea de volumen.

Requisitos previos

- Compruebe que la implementación de OpenStack contiene la imagen, el volumen o la instantánea desde la que desea iniciar la instancia.
- Compruebe que se hayan creado el tipo y la red de la instancia.

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack.
2. En el menú desplegable de la barra de título, seleccione el proyecto.
3. Seleccione **Proyecto > Proceso > Instancias** y haga clic en **Iniciar instancia**.
4. En la página **Detalles**, introduzca la configuración deseada y haga clic en **Siguiente**.

Opción	Descripción
Nombre de la instancia	Introduzca un nombre para la instancia.
Descripción	Introduzca una descripción para la instancia.

Opción	Descripción
Zona de disponibilidad	Seleccione una zona de disponibilidad de Nova en la que se colocará la instancia.
Recuento	Especifique el número de copias de esta instancia que desea crear.

5 En la página **Origen**, seleccione si desea arrancar la instancia desde una imagen, una instantánea de instancia, un volumen o una instantánea de volumen.

   Para instancias que arrancan a partir de imágenes o instantáneas de instancia, puede optar por utilizar almacenamiento persistente mediante la creación de un nuevo volumen. Para instancias que arrancan desde volúmenes o instantáneas de volumen, puede optar por eliminar el volumen o la instantánea especificados cuando se elimina la instancia.

6 En la tabla **Disponible**, seleccione el objeto deseado y haga clic en **Siguiente**.

7 En la página **Tipo**, seleccione el tipo deseado y haga clic en **Siguiente**.

8 En la página **Redes**, seleccione una o varias redes y haga clic en **Siguiente**.

9 En la página **Puertos de red**, seleccione uno o varios puertos y haga clic en **Siguiente**.

   Debe seleccionar al menos una red o al menos un puerto para iniciar la instancia.

10 (opcional) Siga los pasos del asistente para especificar grupos de seguridad, un par de claves, configuraciones personalizadas, grupos de servidores, sugerencias de programador y metadatos.

11 Haga clic en **Iniciar instancia**.

Resultados

La instancia se crea en OpenStack y la máquina virtual correspondiente se crea en vSphere.

Pasos siguientes

En la columna **Acciones**, puede asociar y desasociar interfaces y volúmenes, asociar una dirección IP flotante con la instancia y realizar una serie de acciones adicionales.

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 implementaciones de NSX-T Data Center, consulte Importar máquinas virtuales en VMware Integrated OpenStack con NSX-T Data Center.

Se aplican las siguientes condiciones a máquinas virtuales importadas:

- Si una máquina virtual tiene varios discos, los discos se importan como volúmenes de Cinder.

- Las redes existentes se importan como redes de proveedor basadas en grupos de puertos con acceso restringido al proyecto especificado.
- 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.

Puede importar máquinas virtuales mediante Data Center Command-Line Interface (DCLI) en el cuadro de herramientas de Integrated OpenStack Manager.

Requisitos previos

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

Procedimiento

1 Agregue los clústeres que contengan las máquinas virtuales deseadas como clústeres informáticos de proceso en la implementación de VMware Integrated OpenStack.

Para obtener instrucciones, consulte Agregar clústeres de proceso a la implementación.

2 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

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

a Modifique la configuración del proceso para Nova.

```
viocli update nova-compute
```

b En la sección `vmware`, agregue el parámetro `import_vm_relocate` y establezca el valor como `false`.

Si no realiza este paso, las máquinas virtuales importadas se modificarán de la siguiente manera:

- Los nombres de las máquinas virtuales importadas cambiarán al siguiente formato: *`original-name`* (*`instance-uuid`*)
- Las máquinas virtuales importadas se colocan en la siguiente carpeta de vSphere: *`datacenter`* > *`root-VM-folder`* > OpenStack > Project (*`project-uuid`*)

4 Abra el cuadro de herramientas y conéctese al endpoint de vAPI de VMware Integrated OpenStack.

El endpoint se encuentra en el endpoint de OpenStack privado de la implementación.

```
toolbox
dcli +server http://internal-vip:9449/api +i
```

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`	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`	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`.

Opción	Descripción
`--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] dir/disk_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": "192.0.2.10/24"}, {"mac_address": "00:50:56:9a:ee:be", "ipv4_address": "192.0.2.11/24"}]'`

Resultados

Las máquinas virtuales especificadas se importan en la implementación de OpenStack y se pueden administrar como instancias de OpenStack.

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.

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.

Se aplican las siguientes condiciones a máquinas virtuales importadas:

- 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.

Puede importar máquinas virtuales mediante Data Center Command-Line Interface (DCLI) en el cuadro de herramientas de Integrated OpenStack Manager.

Requisitos previos

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

Procedimiento

1 Agregue los clústeres que contengan las máquinas virtuales deseadas como clústeres informáticos de proceso en la implementación de VMware Integrated OpenStack.

   Para obtener instrucciones, consulte Agregar clústeres de proceso a la implementación.

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 Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

5 Edite la configuración de proceso para Nova.

```
viocli update nova-compute
```

6 En la sección `vmware`, agregue el parámetro `import_net_id` y establezca su valor en el identificador del conmutador que creó.

7 Si desea evitar que las máquinas virtuales importadas cambien de ubicación o de nombre, agregue el parámetro `import_vm_relocate` y establezca su valor en `false`.

8 Abra el cuadro de herramientas y establezca la contraseña de la cuenta de `admin`.

```
toolbox
export OS_PASSWORD=admin-account-password
```

9 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.
--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.

10 Conéctese al endpoint de vAPI de VMware Integrated OpenStack.

El endpoint se encuentra en el endpoint de OpenStack privado de la implementación.

```
dcli +server http://internal-vip:9449/api +i
```

11 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.

Opción	Descripción
`--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] dir/disk_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.

Resultados

La máquina virtual especificada se importa en la implementación de OpenStack y se puede administrar como una instancia de OpenStack.

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.
- Debe desasociar los volúmenes de FCD antes de migrar la instancia.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Si la instancia tiene una unidad de CD-ROM conectada, configure un almacén de datos compartido para la migración de CD-ROM.

   a Edite la configuración de proceso para Nova.

   ```
   viocli update nova-compute
   ```

   b En la sección `vmware`, agregue el parámetro `shared_datastore_regex` y establezca su valor en el nombre del almacén de datos compartido en vSphere.

3 Abra el cuadro de herramientas.

   ```
   toolbox
   ```

4 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.

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 Integrated OpenStack Manager como el usuario `root` y abra el cuadro de herramientas.

```
ssh root@mgmt-server-ip
toolbox
```

2 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.
{--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**).

Resultados

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.

Configurar varios controladores de interfaz virtual

Puede configurar las interfaces virtuales en una instancia de OpenStack para que usen diferentes controladores.

Para especificar los controladores de interfaz virtual, agregue los metadatos `vmware_extra_config` a una imagen de Glance. Todas las interfaces virtuales que no tengan asignado específicamente un controlador en este procedimiento utilizarán el valor de los metadatos `hw_vif_model`. Si no se establecen los metadatos `hw_vif_model`, esas interfaces usarán el controlador predeterminado para la imagen.

Los controladores de interfaz virtual son compatibles con los siguientes valores:

- `e1000`
- `e1000e`
- `pcnet`
- `sriov`
- `vmxnet`
- `vmxnet3`

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack.
2. En el menú desplegable de la barra de título, seleccione el proyecto.
3. Seleccione **Proyecto > Proceso > Imágenes**.
4. Cree una nueva imagen o seleccione una imagen existente en la que desee configurar varios controladores.
5. Seleccione la opción **Actualizar metadatos** que aparece junto a la imagen que desea utilizar.
6. En el campo **Personalizado** en **Metadatos disponibles**, escriba **`vmware_extra_config`** y haga clic en el icono **Agregar** (signo más).
7. Establezca el valor de `vmware_extra_config` en una matriz JSON con el siguiente formato:

   ```
   {"hw_vif_models": {"vif1-id": "driver-name", ...}
   ```

   Por ejemplo, el siguiente valor configura la primera interfaz virtual con el controlador `e1000` y la tercera interfaz virtual con el controlador `vmxnet3`:

   ```
   {"hw_vif_models": {"1": "e1000", "3": "vmxnet3"}
   ```

Habilitar la compatibilidad de página gigante

Las páginas gigantes (conocidas como páginas grandes en Windows) pueden mejorar el rendimiento de algunas cargas de trabajo. VMware Integrated OpenStack admite un tamaño de página máximo de 1 GB.

Requisitos previos

Compruebe que su implementación ejecute vSphere 6.7 o una versión posterior.

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. Configure un tipo para la compatibilidad de página gigante.
   a. Seleccione **Administrador > Proceso > Tipos**.
   b. Cree un nuevo tipo o elija uno existente para utilizarlo en instancias con compatibilidad de página gigante.
   c. Seleccione la opción **Actualizar metadatos** que aparece junto al tipo que desea utilizar.
   d. En el panel **Metadatos disponibles**, expanda **Respaldo de memoria invitada** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Tamaño de página de memoria**.
   e. Establezca el valor de `hw:mem_page_size` en **`grande`**.

      Como alternativa, puede introducir un valor específico con un sufijo de unidad (por ejemplo, **`2 MB`** o **`1GB`**).
   f. En el panel **Metadatos disponibles**, expanda **Cuota de VMware** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Cuota: reserva de memoria en porcentaje**.
   g. Establezca el valor de `quota:memory_reservation_percent` en **`100`** y haga clic en **Guardar**.
4. Configure una imagen para la compatibilidad de página gigante.
   a. Seleccione **Administrador > Proceso > Imágenes**.
   b. Cree una nueva imagen o elija una existente para utilizarla en instancias con compatibilidad de página gigante.
   c. Seleccione la opción **Actualizar metadatos** que aparece junto a la imagen que desea utilizar.
   d. En el panel **Metadatos disponibles**, expanda **Respaldo de memoria invitada** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Tamaño de página de memoria**.

e Establezca el valor de `hw_mem_page_size` en **`grande`**.

Como alternativa, puede introducir un valor específico con un sufijo de unidad (por ejemplo, **`2 MB`** o **`1GB`**).

f En el panel **Metadatos disponibles**, expanda **Cuota de VMware** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Cuota: reserva de memoria en porcentaje**.

g Establezca el valor de `quota_memory_reservation_percent` en **`100`** y haga clic en **Guardar**.

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

Para obtener instrucciones, consulte Iniciar una instancia.

6 Inicie sesión en el sistema operativo invitado de la instancia y habilite la compatibilidad de página gigante.

Para obtener instrucciones, consulte la documentación de su sistema operativo invitado.

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 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 **Proyecto > Proceso > Grupos de servidores**.

4 Haga clic en **Crear grupo de servidores** e introduzca la configuración deseada.

Opción	Descripción
Nombre	Introduzca un nombre para el grupo de servidores.
Directiva	Seleccione la directiva deseada. ■ **Afinidad**: coloca instancias en el mismo host. ■ **Antiafinidad**: coloca instancias en hosts independientes. ■ **Antiafinidad suave**: coloque instancias en hosts distintos si es posible. ■ **Afinidad suave**: coloque instancias en el mismo host, si es posible.

Pasos siguientes

Cuando inicie una instancia, seleccione el grupo de servidores adecuado para implementar afinidad o antiafinidad.

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.

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

Crear una regla de DRS para colocación de instancias de OpenStack

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

Aplicar configuración de grupo de máquinas virtuales a metadatos de imagen

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 **Directivas 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**.

Resultados

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 calidad de servicio para instancias

Para poder controlar las asignaciones de recursos para CPU, memoria, IOPS de disco e interfaces de red virtual, modifique un tipo o una imagen.

Nota No se admite la configuración de cuotas de interfaz virtual en NSX-T Data Center. La configuración de límite, reserva y recursos compartidos de VIF no se puede usar con implementaciones de NSX-T Data Center.

Con el fin de configurar la calidad de servicio para NSX-T Data Center, cree un perfil de Network I/O Control (NIOC) y aplíquelo a la instancia de N-VDS de los nodos de transporte de la implementación. Consulte Configurar perfiles de Network I/O Control.

La asignación de recursos de calidad de servicio también puede especificarse mediante especificaciones adicionales de tipos o metadatos de imagen. Si configuración de tipo y la de imagen entra en conflicto, la configuración de metadatos de imagen tiene prioridad.

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 Especifique un tipo o una imagen que se utilizarán para la calidad de servicio.

- Para utilizar especificaciones adicionales de tipo para la configuración de la calidad de servicio, realice los siguientes pasos:
  a Seleccione **Administrador > Proceso > Tipos**.
  b Cree un nuevo tipo o elija uno existente para utilizarlos para la calidad de servicio.
  c Seleccione la opción **Actualizar metadatos** que aparece junto al tipo que desea utilizar.
- Para utilizar metadatos de imagen en la configuración de la calidad de servicio, realice los siguientes pasos:
  a Seleccione **Administrador > Proceso > Imágenes**.
  b Cree una nueva imagen o elija una existente para utilizarlas para la calidad de servicio.
  c Haga clic en la flecha abajo que aparece junto a la imagen que desea utilizar y seleccione **Actualizar metadatos**.

4 En el panel **Metadatos disponibles**, expanda **Cuota de VMware**.

5 Haga clic en el icono **Agregar** (signo más) junto al elemento que desea usar.

Opción	Descripción
Cuota: límite de CPU	Especifique la asignación máxima de CPU en MHz. El valor `0` indica que el uso de CPU no es limitado.
Cuota: reserva de CPU	Especifique la asignación garantizada de CPU en MHz.
Cuota: reserva de CPU en porcentaje	Especifique la asignación de CPU garantizada como un porcentaje de los ciclos de CPU totales.
Cuota: nivel de recursos compartidos de CPU	Especifique el nivel de recursos compartidos de CPU asignados. Puede introducir **`custom`** y agregar los metadatos de **Cuota: valor de recursos compartidos de CPU** para proporcionar un valor personalizado.
Cuota: valor de recursos compartidos de CPU	Especifique el número de recursos compartidos de CPU asignados. Si los metadatos de **Cuota: nivel de recursos compartidos de CPU** no están establecidos en `custom`, este valor se ignora.
Cuota: límite de E/S de disco	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.
Cuota: reserva de E/S de disco	Especifique la asignación de transacciones de disco garantizadas en E/S por segundo.
Cuota: nivel de recursos compartidos de E/S de disco	Especifique el nivel de recursos compartidos de transacciones de disco asignados. Puede introducir **`custom`** y agregar los metadatos de **Cuota: valor de recursos compartidos de E/S de disco** para proporcionar un valor personalizado.
Cuota: valor de recursos compartidos de E/S de disco	Especifique el número de recursos compartidos de transacciones de disco asignados. Si los metadatos de **Cuota: nivel de recursos compartidos de E/S de disco** no están establecidos en `custom`, este valor se ignora.
Cuota: límite de memoria	Especifique la asignación de memoria máxima en MB. El valor `0` indica que el uso de memoria no es limitado.
Cuota: reserva de memoria	Especifique la asignación de memoria garantizada en MB.
Cuota: reserva de memoria en porcentaje	Especifique la asignación de memoria garantizada como un porcentaje de la memoria total.
Cuota: nivel de recursos compartidos de memoria	Especifique el nivel de recursos compartidos de memoria asignados. Puede introducir **`custom`** y agregar los metadatos de **Cuota: valor de recursos compartidos de memoria** para proporcionar un valor personalizado.
Cuota: valor de recursos compartidos de memoria	Especifique el número de recursos compartidos de memoria asignados. Si los metadatos de **Cuota: nivel de recursos compartidos de memoria** no están establecidos en `custom`, este valor se ignora.
Cuota: límite de VIF	Especifique la asignación máxima de ancho de banda de la interfaz virtual en megabits por segundo (Mbps). El valor `0` indica que el ancho de banda de la interfaz virtual no es limitado.
Cuota: reserva de VIF	Especifique la asignación garantizada de ancho de banda de la interfaz virtual en Mbps.

Opción	Descripción
Cuota: nivel de recursos compartidos de VIF	Especifique el nivel de recursos compartidos de ancho de banda de la interfaz virtual asignados. Puede introducir **`custom`** y los metadatos de **Cuota: valor de recursos compartidos de VIF** para proporcionar un valor personalizado.
Cuota: valor de recursos compartidos de VIF	Especifique el número de recursos compartidos de ancho de banda de la interfaz virtual asignados. Si los metadatos de **Cuota: nivel de recursos compartidos de VIF** no están establecidos en `custom`, este valor se ignora.

6 Haga clic en **Guardar**.

Resultados

Ahora puede implementar instancias habilitadas para la calidad de servicio configurándolas con el tipo o la imagen que modificó en este procedimiento.

Para aplicar la configuración de calidad de servicio a una instancia existente, cambie el tamaño de la instancia y seleccione el tipo con la configuración de calidad de servicio deseada. La configuración especificada se aplica después de que se complete el proceso de cambio de tamaño.

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.

Nota Después de establecer una directiva de almacenamiento en un volumen de FCD, no se puede eliminar la directiva de almacenamiento del volumen. Sin embargo, es posible cambiar la directiva de almacenamiento que utiliza un volumen no asociado.

Requisitos previos

Cree la directiva de almacenamiento que desee en vSphere. Para obtener más información, consulte Administración basada en directivas de almacenamiento en el documento *Almacenamiento de vSphere*.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Edite la configuración de proceso para Nova.

```
viocli update nova-compute
```

a En la sección `DEFAULT`, agregue el parámetro `enabled_filters` con los valores que aparecen en el siguiente ejemplo.

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

b En la sección `vmware`, agregue el parámetro `pbm_default_policy`. Establezca su valor en 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. El valor debe hacer referencia a una directiva de almacenamiento que configure en la vCenter Server.

c En la sección `vmware`, agregue el parámetro `pbm_enabled` y establezca el valor como **`true`**.

d En la sección `vmware`, agregue el parámetro `use_linked_clone` y establezca el valor como **`false`**.

El siguiente ejemplo muestra una configuración actualizada.

```
conf:
nova:
  DEFAULT:
    enabled_filters: "RetryFilter, AvailabilityZoneFilter, RamFilter, ComputeFilter,
ComputeCapabilitiesFilter, ImagePropertiesFilter, ServerGroupAntiAffinityFilter,
ServerGroupAffinityFilter, PciPassthroughFilter, AggregateInstanceExtraSpecsFilter"
  neutron:
    metadata_proxy_shared_secret:
".Secret:managedencryptedpasswords:data.metadata_proxy_shared_secret"
  vmware:
    passthrough: "false"
    pbm_default_policy: "Your Default Storage Policy"
    pbm_enabled: "true"
    tenant_vdc: "false"
    use_linked_clone: "false"
```

3 Edite la configuración de Nova.

```
viocli update nova
```

a En la sección `DEFAULT`, agregue el parámetro `enabled_filters` con los valores que aparecen en el siguiente ejemplo.

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

b En la sección `vmware`, agregue el parámetro `pbm_default_policy`. Establezca su valor en 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. El valor debe hacer referencia a una directiva de almacenamiento que configure en la vCenter Server.

c En la sección `vmware`, agregue el parámetro `pbm_enabled` y establezca el valor como **`true`**.

d En la sección `vmware`, agregue el parámetro `use_linked_clone` y establezca el valor como **`false`**.

El siguiente ejemplo muestra una configuración actualizada.

```
conf:
nova:
  DEFAULT:
    enabled_filters: "RetryFilter, AvailabilityZoneFilter, RamFilter, ComputeFilter,
ComputeCapabilitiesFilter, ImagePropertiesFilter, ServerGroupAntiAffinityFilter,
ServerGroupAffinityFilter, PciPassthroughFilter, AggregateInstanceExtraSpecsFilter"
  neutron:
    metadata_proxy_shared_secret:
".Secret:managedencryptedpasswords:data.metadata_proxy_shared_secret"
  vmware:
    passthrough: "false"
    pbm_default_policy: "Your Default Storage Policy"
    pbm_enabled: "true"
    tenant_vdc: "false"
    use_linked_clone: "false"
```

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

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

6 Seleccione **Administrador > Proceso > Tipos**.

7 Cree un nuevo tipo o elija uno existente.

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

9 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**.

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

Resultados

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.

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**, seleccione y configure los metadatos necesarios.

   a Expanda **Asignación de CPU** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Directiva de asignación de la CPU** .

   b Establezca el valor de `hw:cpu_policy` en **`dedicated`**.

   c Expanda **Directivas de VMware** y haga clic en el icono **Agregar** (signo más) que aparece junto a **Sensibilidad de latencia de máquina virtual**.

   d Establezca el valor de `vmware:latency_sensitivity_level` en **`high`**.

   e Expanda **Cuota de VMware** y haga clic en el icono **Agregar** (signo más) junto a **Reserva de CPU en porcentaje** y **Reserva de memoria en porcentaje**.

   f Establezca el valor de `quota:cpu_reservation_percent` y `quota:memory_reservation_percent` en **`100`**.

7 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.

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 Utilizar 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 Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Abra el cuadro de herramientas y establezca la contraseña de la cuenta de `admin`.

```
toolbox
export OS_PASSWORD=admin-account-password
```

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 el acceso directo para los dispositivos de redes

Puede configurar un puerto para permitir el acceso directo de SR-IOV y, a continuación, crear instancias de OpenStack que usen adaptadores de red física.

Importante Esta función solo está disponible en VMware Integrated OpenStack Carrier Edition. Para obtener más información, consulte Licencias de VMware Integrated OpenStack.

Requisitos previos

- Habilite SR-IOV en vSphere. Consulte Habilitar SR-IOV en un adaptador físico de 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.
- Habilite las funciones de VMware Integrated OpenStack Carrier Edition. Consulte Habilitar funciones de Carrier Edition.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Edite la configuración de proceso para Nova.

```
viocli update nova-compute
```

3 Añada la siguiente información en la sección `nova_compute`.

```
pci:
  passthrough_whitelist:
    type: multistring
    values:
    - '{"product_id": "*", "vendor_id": "*", "physical_network": "*"}'
```

4 Si utiliza una implementación de NSX-T Data Center, agregue el parámetro `dvs_moid` en la sección `vmware`.

```
dvs_moid: sriov-vds-moid
```

Establezca el valor de `dvs_moid` como el identificador de objeto administrado (Managed Object Identifier, MOID) del conmutador distribuido asociado con el clúster de proceso para dispositivos de SR-IOV.

5 Abra el cuadro de herramientas y establezca la contraseña de la cuenta de `admin`.

```
toolbox
export OS_PASSWORD=admin-password
```

6 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 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.

7 Cree una subred en la red externa.

```
neutron subnet-create network-id --tenant-id project-uuid --name subnet-name
```

Opción	Descripción
network-id	Especifique el UUID de la red en la que se va a crear la subred. 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 la subred.
`--name`	Introduzca un nombre para la subred.

8 Cree un puerto habilitado para acceso directo mediante el parámetro `--vnic_type direct`.

```
neutron port-create network-id --tenant-id project-uuid --name port-name --vnic_type direct
```

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.

Nota La seguridad del puerto no es compatible con puertos habilitados para acceso directo, y se deshabilitará automáticamente para el puerto que se creó.

Resultados

Puede configurar instancias con el puerto creado en este procedimiento para permitirles utilizar dispositivos de SR-IOV.

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

Puede configurar un tipo para permitir el acceso directo y, a continuación, crear instancias de OpenStack que usen interfaces de hardware físico.

Este procedimiento no se aplica a las vGPU NVIDIA GRID. Para configurar una vGPU NVIDIA GRID, consulte Configurar el acceso directo para un vGPU NVIDIA GRID.

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 el 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.
- Compruebe que los metadatos `vmware_extra_config` no estén configurados en la imagen que desea utilizar para el acceso directo.
- 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 Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Edite la configuración de Nova.

```
viocli update nova
```

3 En la sección `nova`, cree la sección `DEFAULT`. En la sección `DEFAULT`, cree la sección `pci_alias`.

4 En la sección `pci_alias`, agregue el parámetro `type` y establezca el valor como `multistring`.

5 Agregue el parámetro `values` y establezca su valor para que coincida con su dispositivo.

Use el siguiente formato:

```
values:
- '{"device_type": "type-PF", "vendor_id": "vendor-id", "name": "physical-name"}'
- '{"device_type": "type-VF", "vendor_id": "vendor-id", "name": "virtual-name"}'
```

Opción	Descripción
vendor-id	Introduzca el identificador de proveedor de cuatro caracteres para el dispositivo. Escriba todas las letras en minúscula.
physical-name	Introduzca un alias para el dispositivo físico.
virtual-name	Introduzca un alias para el dispositivo virtual.

6 En la sección `vmware`, agregue el parámetro `generic_passthrough` y establezca el valor como **`true`**.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  nova:
    vmware:
      [...]
      generic_passthrough: true
```

```
    DEFAULT:
      pci_alias:
        type: multistring
        values:
        - '{"device_type": "type-PF", "vendor_id": "vendor-id", "name": "physical-name"}'
        - '{"device_type": "type-VF", "vendor_id": "vendor-id", "name": "virtual-name"}'
```

7 Edite la configuración de proceso para Nova.

```
viocli update nova-compute
```

8 En la sección `vmware`, agregue el parámetro `generic_passthrough` y establezca el valor como **`true`**.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  nova_compute:
    DEFAULT:
      [...]
    vmware:
      [...]
      generic_passthrough: true
```

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

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

11 Seleccione **Administrador > Proceso > Tipos**.

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

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

14 En el campo **Personalizado** en **Metadatos disponibles**, escriba **`vmware_extra_config`** y haga clic en el icono **Agregar** (signo más).

15 Establezca el valor de `vmware:extra_config` en **`{"pciPassthru.use64bitMMIO":"TRUE"}`**.

16 En el campo **Personalizado** en **Metadatos disponibles**, escriba **`pci_passthrough:alias`** y haga clic en el icono **Agregar** (signo más).

17 Establezca el valor de `pci_passthrough:alias` en *`virtual-device-name`*:*`device-count`*.

Opción	Descripción
virtual-device-name	Introduzca el nombre del dispositivo virtual que especificó en 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.

18 Expanda **Cuota de VMware** y haga clic en el icono **Agregar** (signo más) que aparece junto a `Quota: Memory Reservation`.

19 Establezca el valor de `quota:memory_reservation` en **`100`** y haga clic en **Guardar**.

Resultados

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

Configurar el acceso directo para un vGPU NVIDIA GRID

Puede permitir que una instancia de OpenStack use un dispositivo de vGPU NVIDIA GRID en su host ESXi.

Nota

- Solo se admite un vGPU por instancia de OpenStack.
- Se utiliza el mismo perfil de vGPU para todas las instancias de OpenStack.

Requisitos previos

Compruebe que el controlador para el dispositivo de vGPU esté instalado en el host ESXi.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Edite la configuración de proceso para Nova.

```
viocli update nova-compute
```

3 En la sección `vmware`, agregue el parámetro `gpu_profile` y establezca su valor como el perfil de vGPU que desea utilizar.

Por ejemplo:

```
nova_gpu_profile: gpu_profile
```

4 Agregue el parámetro `profile_fb_size_kb` y establezca su valor como el tamaño del búfer de trama de vGPU en megabytes (MB).

Por ejemplo, introduzca `profile_fb_size_kb: 4096` para indicar un búfer de trama de 4.096 MB.

Para obtener más información sobre búferes de trama, consulte la Guía del usuario del software de GPU virtual de NVIDIA.

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

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

7 Seleccione **Administrador > Proceso > Tipos**.

8 Cree un nuevo tipo o elija uno existente para utilizarlos para el acceso directo de vGPU NVIDIA GRID.

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

10 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 a **vGPU de VMware**.

11 Establezca el valor de `vmware:vgpu` en `1` y haga clic en **Guardar**.

Pasos siguientes

Ahora puede configurar una instancia para utilizar vGPU NVIDIA GRID mediante la configuración de la instancia con el tipo que modificó en este procedimiento.

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.

Nota No se admite la configuración de cuotas de interfaz virtual en NSX-T Data Center. Las siguientes especificaciones adicionales no se pueden utilizar con implementaciones de NSX-T Data Center:

- `quota:vif_limit`
- `quota:vif_reservation`
- `quota:vif_shares_level`
- `quota:vif_shares_share`

Con el fin de configurar la calidad de servicio para NSX-T Data Center, cree un perfil de Network I/O Control (NIOC) y aplíquelo a la instancia de N-VDS de los nodos de transporte de la implementación. Consulte Configurar perfiles de Network I/O Control.

Si hay un conflicto entre los metadatos de imagen y la especificación adicional de tipo, los metadatos de imagen tienen prioridad sobre la especificación adicional de tipo.

Tabla 5-1. Especificaciones adicionales de tipos en VMware Integrated OpenStack

Especificación adicional	Descripción
`hw:vifs_multi_thread`	Especifique **`true`** para proporcionar a cada interfaz virtual su propio subproceso de transmisión.
`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`	Especifique la asignación garantizada de CPU en MHz.

Tabla 5-1. Especificaciones adicionales de tipos en VMware Integrated OpenStack (continuación)

Especificación adicional	Descripción
`quota:cpu_reservation_percent`	Especifique 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`	Especifique 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`	Especifique el número de recursos compartidos de CPU asignados. Si no se establece el parámetro `cpu_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`	Especifique 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`	Especifique 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: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`	Especifique 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`	Especifique el número de recursos compartidos de memoria asignados. Si no se establece el parámetro `memory_shares_level` como `custom`, se omite este valor.

Tabla 5-1. Especificaciones adicionales de tipos en VMware Integrated OpenStack (continuación)

Especificación adicional	Descripción
`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.
`quota:vif_reservation`	Especifique la asignación garantizada de ancho de banda de la interfaz virtual en Mbps.
`quota:vif_shares_level`	Especifique 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`	Especifique el número de recursos compartidos de ancho de banda de la interfaz virtual asignados. Si no se establece el parámetro `vif_shares_level` como `custom`, se omite este valor.
`vmware:boot_efi_secure_boot`	Especifique **`true`** para realizar comprobaciones de firmas en cualquier imagen de EFI que se cargue durante el inicio.
`vmware:boot_enter_bios`	Especifique **`true`** para que las máquinas virtuales entren en la configuración del BIOS durante el siguiente inicio. Las máquinas virtuales restablecen este parámetro automáticamente después del siguiente inicio.
`vmware:boot_retry`	Especifique el retraso en milisegundos antes de que se inicie la secuencia de arranque.
`vmware:boot_retry_delay`	Especifique el retraso en milisegundos antes de que se vuelva a intentar la secuencia de arranque. Si se establece el parámetro `boot_retry_enabled` como `false`, se omite este valor.
`vmware:boot_retry_enabled`	Especifique **`true`** para volver a intentar la secuencia de arranque si se produce un error en el arranque.
`vmware:cpu_affinity`	Especifique una lista de las CPU que pueden utilizar las instancias.
`vmware:extra_config`	Especifique las configuraciones personalizadas en formato JSON. Por ejemplo, `'{"acpi.smbiosVersion2.7":"FALSE"}'`.
`vmware:hw_version`	Especifique la versión de hardware que se utiliza para crear imágenes. En un entorno con versiones de host diferentes, puede usar este parámetro para colocar instancias en los hosts correctos.
`vmware:latency_sensitivity_level`	Especifique el nivel de sensibilidad de latencia para las máquinas virtuales.

Tabla 5-1. Especificaciones adicionales de tipos en VMware Integrated OpenStack (continuación)

Especificación adicional	Descripción
`vmware:resource_pool`	Especifique el grupo de recursos en el que se colocarán las nuevas instancias. Si el nombre del proyecto que contiene la instancia coincide con el nombre de un grupo de recursos del entorno, la instancia se colocará en ese grupo de recursos de forma predeterminada. Si se establece este parámetro, se anula el comportamiento predeterminado y se fuerza a que la instancia se coloque en el grupo de recursos especificado.
`vmware:set_bios_uuid`	Especifique **`true`** para utilizar el UUID de Nova de las instancias como el UUID del dispositivo.
`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:vgpu`	Especifique el número de vGPU compartidas que se asociarán a la instancia.
`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.

Volúmenes y tipos de volumen de Cinder

6

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. Los usuarios de la nube pueden asociar un volumen a una instancia en ejecución, o bien desasociar un volumen y asociarlo a otra instancia.

Para obtener más información sobre Cinder, consulte la Documentación de OpenStack Cinder.

Este capítulo incluye los siguientes temas:

- Create a Volume
- Crear un volumen con capacidades de asociación múltiple
- Transferir un volumen
- Crear un tipo de volumen
- Manage a Volume
- Migración de volúmenes entre almacenes de datos
- Especificaciones adicionales de tipos de volúmenes compatibles

Create a Volume

You create volumes and attach them to instances to provide persistent storage.

Requisitos previos

- If you want to create a volume from an image, upload the desired image. See Importar una imagen.
- If you want to create an FCD-backed volume, verify that you have added at least one Cinder host using the FCD back end. Then create a volume type and set its `vmware:backend_name` extra spec to the name of the FCD back end. Select this volume type during the volume creation process. For information about volume types, see Crear un tipo de volumen.

Procedimiento

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

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

3 Select **Project > Volumes > Volumes**.

4 Click **Create Volume** and enter the desired configuration.

Option	Description
Volume Name	Enter a name for the new volume.
Description	Enter a description for the volume.
Volume Source	Select **No source, empty volume**, **Snapshot**, **Image**, or **Volume**. If you select **Snapshot**, **Image**, or **Volume**, specify the desired object from the next drop-down menu.
Type	If you selected **No source, empty volume** or **Image** as the volume source, select a volume type for the volume. For volumes whose source is a volume snapshot or another volume, the volume type is inherited from the source.
Size (GiB)	Enter the size of the volume in gibibytes.
Availability Zone	If you selected **No source, empty volume** or **Image** as the volume source, specify the availability zone in which to create the volume. For volumes whose source is a volume snapshot or another volume, the availability zone is inherited from the source.

5 Click **Create Volume**.

Pasos siguientes

In the **Actions** column to the right of the volume, you can perform the following actions:

- Click **Edit Volume** to modify the name and description of the volume and whether it is bootable.
- Click **Extend Volume** to increase the size of an unattached volume.
- Click **Launch as Instance** to create an instance using an unattached volume.
- Click **Manage Attachments** to attach the volume to or detach the volume from an instance.
- Click **Create Snapshot** to take a snapshot of the volume.

  Nota Creating a snapshot of a volume attached to an instance can result in a corrupted snapshot. If possible, detach the volume before creating the snapshot.

- Click **Change Volume Type** to modify the volume type and migration policy.
- Click **Upload to Image** to upload the volume to Glance as an image.
- Click **Create Transfer** to assign ownership of an unattached volume to a different project. For details, see Transferir un volumen.

- Click **Update Metadata** to add, remove, or change volume metadata.

You can also select one or more unattached volumes and click **Delete Volumes** to remove them.

Crear un volumen con capacidades de asociación múltiple

Con la asociación múltiple de Cinder, puede asociar volúmenes simultáneamente a varias instancias.

Requisitos previos

Si desea usar volúmenes de asociación múltiple, tenga en cuenta las siguientes limitaciones:

- Se requiere aceleración de hardware para almacenes de datos de NFS que respaldan volúmenes de asociación múltiple.
- Los volúmenes de asociación múltiple no se pueden reubicar mientras están en uso. Para evitar los efectos de esta limitación, cree volúmenes de asociación múltiple en un almacén de datos compartido.

  Puede especificar almacenes de datos para volúmenes de asociación múltiple mediante un perfil de almacenamiento. Cree el perfil de almacenamiento deseado en vSphere y asígnelo al tipo de volumen definido en este procedimiento mediante la especificación adicional de `vmware:storage_profile`.
- Los volúmenes de asociación múltiple deben usar la puesta a cero rápida con aprovisionamiento grueso como formato de aprovisionamiento.
- Los volúmenes de asociación múltiple deben utilizar VMDK como controlador de back-end. Los volúmenes de FCD no admiten asociación múltiple.
- Para evitar daños en los datos, formatee los volúmenes de asociación múltiple con un sistema de archivos consciente del clúster.
- No puede clonar, realizar una copia de seguridad o tomar instantáneas de volúmenes de asociación múltiple mientras estos volúmenes estén conectados.
- Si más de ocho hosts ESXi intentan acceder a un solo volumen de asociación múltiple de forma simultánea, se producirá un error al conectar el volumen.
- No se puede realizar una migración en vivo en una instancia a la que se ha conectado un volumen de asociación múltiple.
- El comando `viocli prepare datastore` no admite volúmenes de asociación múltiple. Desasocie los volúmenes de asociación múltiple antes de migrarlos a otro almacén de datos.

Procedimiento

1. Cree un nuevo tipo de volumen o elija un tipo de volumen existente para utilizar para asociación múltiple.

   Para obtener instrucciones, consulte Crear un tipo de volumen.
2. Seleccione **Ver especificaciones adicionales** junto al tipo de volumen que desea utilizar.

3 Haga clic en **Crear**.

4 En el campo **Clave**, introduzca **`multiattach`**.

5 En el campo **Valor**, introduzca **`<is> True`**.

6 Haga clic en **Crear**.

7 En la página **Especificaciones adicionales de tipo de volumen**, haga clic en **Crear**.

8 En el campo **Clave**, introduzca **`vmware:vmdk_type`**.

9 En el campo **Valor**, introduzca **`eagerZeroedThick`**.

10 Haga clic en **Crear**.

11 (opcional) Especifique un perfil de almacenamiento para garantizar que los volúmenes de asociación múltiple se creen en almacenes de datos admitidos.

   a En la página **Especificaciones adicionales de tipo de volumen**, haga clic en **Crear**.

   b En el campo **Clave**, introduzca **`vmware:storage_profile`**.

   c En el campo **Valor**, introduzca el nombre del perfil de almacenamiento deseado.

   d Haga clic en **Crear**.

Resultados

Se creará un tipo de volumen con capacidades de asociación múltiple. Para crear volúmenes de asociación múltiple, seleccione este tipo de volumen al crear o volver a escribir volúmenes. Tenga en cuenta que la reescritura de un volumen para habilitar o deshabilitar la asociación múltiple solo se admite cuando el volumen está desconectado.

Transferir un volumen

Puede asignar la propiedad de un volumen no asociado a otro proyecto.

Requisitos previos

Asegúrese de que el volumen que desea transferir no se asoció a ninguna instancia.

Procedimiento

- Para iniciar una transferencia, siga estos pasos:

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

   b En el menú desplegable de la barra de título, seleccione el proyecto.

   c Seleccione **Proyecto > Proceso > Volúmenes**.

   d En la columna **Acciones** junto al volumen que desea transferir, haga clic en **Crear transferencia**.

e Introduzca un nombre para la tarea de transferencia y haga clic en **Crear transferencia de volumen**.

f Registre o descargue la clave de autorización y el identificador de transferencia que se muestran en la página **Detalles de la transferencia de volumen** y envíe esta información al usuario que aceptará la transferencia.

Importante Después de cerrar la página **Detalles de la transferencia de volumen**, ya no se podrán recuperar la clave de autorización y el identificador de transferencia. Si se pierden la clave de autorización o el identificador de transferencia, debe cancelar la transferencia e iniciarla de nuevo.

- Para recibir una transferencia, siga estos pasos:

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

  b En el menú desplegable de la barra de título, seleccione el proyecto.

  c Seleccione **Proyecto > Proceso > Volúmenes** y haga clic en **Aceptar transferencia**.

  d Introduzca la clave de autorización y el identificador de transferencia que recibió del usuario que inició la transferencia.

  e Haga clic en **Aceptar transferencia de volumen**.

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 volúmenes pueden definir un perfil de almacenamiento de vSphere y un tipo de adaptador predeterminado.

Nota No se admite el cifrado de Barbican para volúmenes o tipos de 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 > 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 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**.

8 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**.

9 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.

Resultados

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**.

Manage a Volume

You can manage non-OpenStack volumes on the Cinder hosts in your deployment. Managing a volume makes it usable in your OpenStack deployment.

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 Select **Admin > Volume > Volumes**.

4 Click **Manage Volume** and enter the desired configuration.

Option	Description
Identifier	Enter the name or identifier for the source volume. **Nota** To migrate a volume from the VMDK back end to the FCD back end, enter the ID of the existing VMDK volume.
Identifier Type	Select **Name** or **ID**. **Nota** To migrate a volume from the VMDK back end to the FCD back end, select **ID**.
Host	Enter the Cinder host that contains the existing volume. Use the following format: *`host:backend-name@pool`*.
Volume Name	Enter a name for the volume.
Description	Enter a description of the volume.
Metadata	Enter metadata as key-value pairs. For example, `img_config_drive=mandatory`.
Volume Type	Select a volume type for the volume.
Availability Zone	Select an availability zone in which to place the volume.
Bootable	Select the checkbox to allow instances to boot from the volume.

5 Click **Manage**.

Resultados

The specified volume is managed by Cinder and visible in 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.

Nota No se puede migrar un volumen que tenga instantáneas asociadas. Debe desasociar todas las instantáneas antes de migrar un volumen.

Migrar todos los volúmenes de un almacén de datos

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.
- En el clúster de almacenes de datos, habilite Storage DRS y establézcalo en **Sin automatización (modo manual)**.
- Desasocie todas las instantáneas de todos los volúmenes del almacén de datos.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Prepare los volúmenes del almacén de datos para la migración.

```
viocli prepare datastore dc-name ds-name
```

Opción	Descripción
dc-name	Introduzca el nombre del centro de datos que contiene el almacén de datos deseado.
ds-name	Introduzca el nombre del almacén de datos.

3 Coloque el almacén de datos en modo de mantenimiento.

Consulte Poner un almacén de datos en modo de mantenimiento en el documento *Administrar recursos de vSphere*.

Resultados

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

Desasocie todas las instantáneas de los volúmenes que desea migrar.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Migre los volúmenes.

- Para migrar todos los volúmenes de un almacén de datos, ejecute el siguiente comando:

```
viocli migrate volume --source-dc src-dc-name --source-ds src-ds-name dest-dc-name dest-ds-name [--ignore-storage-policy]
```

- Para migrar volúmenes especificados de un almacén de datos, ejecute el siguiente comando:

```
viocli migrate volume --volume-ids UUID1 dest-dc-name dest-ds-name [--ignore-storage-policy]
```

Opción	Descripción
--source-dc	Introduzca el centro de datos que contiene los volúmenes que desea migrar. Este parámetro debe utilizarse junto con el parámetro --source-ds. Si solo desea migrar volúmenes especificados, no incluya este parámetro.
--source-ds	Introduzca el almacén de datos que contiene los volúmenes que desea migrar. Este parámetro debe utilizarse junto con el parámetro --source-dc. Si solo desea migrar volúmenes especificados, no incluya este parámetro.
--volume-ids	Introduzca el UUID del volumen que desea migrar. Puede incluir varios UUID, separados por comas (,). Si desea migrar todos los volúmenes de un almacén de datos, use los parámetros --source-dc y --source-ds en lugar de este parámetro.
dest-dc-name	Introduzca el nombre del centro de datos que contiene el almacén de datos al que desea migrar volúmenes.
dest-ds-name	Introduzca el nombre del almacén de datos al que desea migrar volúmenes.
--ignore-storage-policy	Incluya este parámetro para migrar volúmenes al almacén de datos de destino, incluso si el almacén de datos no cumple con la directiva de almacenamiento del volumen.

Resultados

Los volúmenes especificados se migran al almacén de datos de destino.

Migrar volúmenes Cinder asociados

Puede migrar volúmenes de Cinder asociados a una instancia de OpenStack mediante la migración de la máquina virtual correspondiente a un almacén de datos diferente.

Nota

- Los volúmenes de asociación múltiple no se pueden migrar mientras estén asociados. Desasocie los volúmenes de asociación múltiple antes de migrarlos a otro almacén de datos.
- Después de migrar un volumen asociado, la máquina virtual de sombra correspondiente permanece en el almacén de datos original, pero no tiene ningún disco. Al desasociar el volumen, el disco se volverá a conectar con la máquina virtual de sombra.

Requisitos previos

Desasocie todas las instantáneas de los volúmenes que desea migrar.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Prepare el almacén de datos que contiene el volumen para la migración.

Este paso prepara todos los volúmenes del almacén de datos especificado para la migración.

```
viocli prepare datastore 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.

3 Abra el cuadro de herramientas.

```
toolbox
```

4 Migre la instancia a la que está asociado el volumen.

```
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**.

Para obtener más información, consulte Migrar una instancia.

5 En vSphere Client, migre la máquina virtual correspondiente a la instancia de OpenStack a la que está asociado el volumen.

Para obtener información, consulte Migrar una máquina virtual a un almacenamiento nuevo en vSphere Web Client.

6 Si desea migrar la máquina virtual de sombra a un clúster en una zona de disponibilidad diferente, actualice el host Cinder para el volumen.

a Obtenga una lista de los pods de cinder-api en el nodo LCM.

```
osctl get pods | grep cinder-api
```

b Con el nombre de uno de los pods cinder-api que se muestra, inicie una sesión de bash en el pod.

```
osctl exec -it <cinder-api-pod-name> bash
```

c En la nueva sesión, obtenga una lista de hosts Cinder.

```
cinder-manage host list
```

La lista incluye los hosts y las zonas de los volúmenes de Cinder.

d Modifique los atributos del volumen que desea mover. Establezca los valores del host y la zona en el host de volumen Cinder en la zona de disponibilidad en la que desea mover la máquina virtual de sombra.

```
cinder-manage volume update volume_host --volume_id <volume-uuid> --newhost <new-volume-host>
--zone <availability-zone>
```

Donde:

- *volumen-UUID* es el UUID del volumen Cinder de la máquina virtual de sombra que se desea mover.
- *new-volume-host* es el nombre de host Cinder en la zona de disponibilidad del destino.
- *availability-zone* es la zona de disponibilidad de destino.

Resultados

El volumen de Cinder y el disco de la máquina virtual de sombra correspondiente se migran al nuevo almacén de datos.

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 6-1. 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 7

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.

VMware Integrated OpenStack no es compatible con los comandos **`openstack image save`** y **`glance image-download`**.

Este capítulo incluye los siguientes temas:

Importar una imagen

Puede importar un archivo de imagen en la implementación de VMware Integrated OpenStack y utilizarlo para iniciar instancias.

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.
2. En el menú desplegable de la barra de título, seleccione el proyecto.
3. Seleccione **Proyecto > Proceso > Imágenes**.
4. Haga clic en **Crear imagen** e introduzca la configuración deseada.

Opción	Acción
Nombre de la imagen	Introduzca un nombre para la imagen.
Descripción de la imagen	Introduzca una descripción para la imagen.
Origen de la imagen	Haga clic en **Examinar** y 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	(Solo administradores de nube) 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

Ahora puede iniciar instancias a partir de la imagen. En la columna **Acciones** junto a una imagen, puede editar o eliminar la imagen, actualizar sus metadatos, iniciar una instancia desde la imagen o crear un volumen a partir de la imagen.

Importar una plantilla de máquina virtual como imagen

Puede agregar plantillas de máquina virtual a la implementación de VMware Integrated OpenStack como imágenes de Glance.

Requisitos previos

- Compruebe que la plantilla de máquina virtual esté en la misma instancia de vCenter Server que la implementación de VMware Integrated OpenStack.

- Compruebe que la plantilla de máquina virtual no tenga varios discos, una unidad de CD-ROM o una unidad de disquete.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Abra el cuadro de herramientas y establezca la contraseña de la cuenta de `admin`.

```
toolbox
export OS_PASSWORD=admin-account-password
```

3 Cree una imagen de Glance vacía en formato VMDK.

```
glance image-create --name image-name --disk-format vmdk --container-format bare
```

4 Agregue la ubicación de la plantilla de máquina virtual a la imagen.

```
glance location-add image-uuid --url vi://vcserver-ip/datacenter-name/vm/folder-name/template-name
```

Puede revisar la **Vista de máquina virtual y plantillas** en vSphere Client para confirmar la ubicación de la plantilla.

Resultados

La plantilla de máquina virtual especificada se importa como una imagen. Puede iniciar instancias de OpenStack desde la imagen o configurar opciones adicionales, como metadatos de imagen.

Migrar una imagen

Puede migrar una imagen a otro almacén de datos y, a la vez, preservar su UUID y metadatos.

Requisitos previos

Determine el UUID de la imagen que desea migrar y del proyecto que contiene la imagen. Puede usar el comando `openstack image list` para mostrar el UUID de cada imagen y el comando `openstack image show` para mostrar el UUID del proyecto que contiene una imagen especificada.

Procedimiento

1 En vSphere Client, abra las **máquinas virtuales y plantillas**, vea y busque la imagen que desea migrar.

La imagen se encuentra en la carpeta del proyecto que la contiene.

2 Haga clic con el botón secundario en la imagen y seleccione **Clonar a plantilla**.

3 Introduzca un nuevo nombre para la imagen y haga clic en **Siguiente**.

4 Seleccione el recurso informático deseado y haga clic en **Siguiente**.

5 Seleccione el almacén de datos deseado y haga clic en **Siguiente**.

6 Haga clic en **Finalizar**.

7 Registre el nombre de la imagen original como se muestra en vSphere.

8 Elimine la imagen original.

9 Cambie el nombre de la imagen clonada al nombre de la imagen original.

Resultados

La imagen se mueve al nuevo almacén de datos. Puede seguir iniciando instancias a partir de ella de forma normal.

Configurar una imagen para la personalización de invitado de Windows

Puede configurar imágenes para la personalización de invitado de Windows mediante la aplicación de metadatos de la personalización de invitado.

La personalización de invitado de Windows es una alternativa a Cloudbase-Init. No utilice los metadatos de personalización de invitado de Windows y Cloudbase-Init en la misma imagen.

Requisitos previos

- Instale la versión adecuada de Microsoft System Preparation (Sysprep) para cada sistema operativo invitado que desea personalizar.
- Instale VMware Tools en la imagen de origen.

Procedimiento

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

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

3 Seleccione **Proyecto > Proceso > Imágenes**.

4 Cree una nueva imagen de Windows o elija una imagen existente para personalizarla.

5 Seleccione la opción **Actualizar metadatos** que aparece junto a la imagen que desea utilizar.

6 En el panel **Metadatos disponibles**, expanda **Opciones de personalización de invitado**.

7 Haga clic en el icono **Agregar** (signo más) junto a los metadatos que desea configurar.

Opción	Descripción
Conteo de inicio de sesión automático	Introduzca la cantidad de veces que la máquina puede iniciar sesión automáticamente como administrador. Puede aumentar este valor por encima de 1 si la configuración requiere varios reinicios. Este valor se puede determinar mediante la lista de comandos ejecutados por el comando `GuiRunOnce`.
Inicio de sesión automático	Seleccione la casilla de verificación para iniciar sesión automáticamente en la máquina virtual como administrador.
Cantidad máxima de conexiones	Escriba el número de licencias de cliente adquiridas para el servidor de Windows que se va a instalar. **Nota** Este parámetro se utiliza únicamente si el modo de licencia de servidor está establecido en `PerServer`.
Clave del producto	Introduzca el número de serie para incluirlo en el archivo de respuesta cuando se ejecuta mini-setup. **Nota** Si el sistema operativo invitado se instaló mediante un CD para licencias por volumen, este parámetro no es necesario.
Modo de licencias de servidor	Seleccione **PerServer** o **PerSeat** como el modo de licencia de servidor.
Grupo de trabajo de Windows al cual unirse	Seleccione el grupo de trabajo al que se unirá la máquina virtual.

8 Haga clic en **Guardar**.

Resultados

Al iniciar instancias a partir de la imagen, se aplican las opciones de personalización de invitado de Windows que se especificaron.

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.

Nota No se admite la configuración de cuotas de interfaz virtual en NSX-T Data Center. Los siguientes metadatos no se pueden utilizar con implementaciones de NSX-T Data Center:

- `quota_vif_limit`
- `quota_vif_reservation`
- `quota_vif_shares_level`
- `quota_vif_shares_share`

Con el fin de configurar la calidad de servicio para NSX-T Data Center, cree un perfil de Network I/O Control (NIOC) y aplíquelo a la instancia de N-VDS de los nodos de transporte de la implementación. Consulte Configurar perfiles de Network I/O Control.

Si hay un conflicto entre los metadatos de imagen y la especificación adicional de tipo, los metadatos de imagen tienen prioridad sobre la especificación adicional de tipo.

Tabla 7-1. Metadatos de imagen en VMware Integrated OpenStack

Especificación adicional	Descripción
`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`	Especifique la asignación garantizada de CPU en MHz.
`quota_cpu_reservation_percent`	Especifique 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`	Especifique 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`	Especifique el número de recursos compartidos de CPU asignados. Si no se establece el parámetro `cpu_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.

Tabla 7-1. Metadatos de imagen en VMware Integrated OpenStack (continuación)

Especificación adicional	Descripción
quota_disk_io_shares_level	Especifique 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	Especifique 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_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	Especifique 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	Especifique el número de recursos compartidos de memoria asignados. Si no se establece el parámetro memory_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.
quota_vif_reservation	Especifique la asignación garantizada de ancho de banda de la interfaz virtual en Mbps.
quota_vif_shares_level	Especifique 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	Especifique 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.
vmware_boot_efi_secure_boot	Especifique **true** para realizar comprobaciones de firmas en cualquier imagen de EFI que se cargue durante el inicio.
vmware_boot_enter_bios	Especifique **true** para que las máquinas virtuales entren en la configuración del BIOS durante el siguiente inicio. Las máquinas virtuales restablecen este parámetro automáticamente después del siguiente inicio.

Tabla 7-1. Metadatos de imagen en VMware Integrated OpenStack (continuación)

Especificación adicional	Descripción
vmware_boot_retry	Especifique el retraso en milisegundos antes de que se inicie la secuencia de arranque.
vmware_boot_retry_delay	Especifique el retraso en milisegundos antes de que se vuelva a intentar la secuencia de arranque. Si se establece el parámetro boot_retry_enabled como false, se omite este valor.
vmware_boot_retry_enabled	Especifique **true** para volver a intentar la secuencia de arranque si se produce un error en el arranque.
vmware_cpu_affinity	Especifique una lista de las CPU que pueden utilizar las instancias.
vmware_extra_config	Especifique las configuraciones personalizadas en formato JSON. Por ejemplo, '{"acpi.smbiosVersion2.7":"FALSE"}'.
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_resource_pool	Especifique el grupo de recursos en el que se colocarán las nuevas instancias. Si el nombre del proyecto que contiene la instancia coincide con el nombre de un grupo de recursos del entorno, la instancia se colocará en ese grupo de recursos de forma predeterminada. Si se establece este parámetro, se anula el comportamiento predeterminado y se fuerza a que la instancia se coloque en el grupo de recursos especificado.
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_vgpu	Especifique el número de vGPU compartidas que se asociarán a la instancia.
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.

Orquestación y pilas de Heat

8

Puede usar pilas de Heat para automatizar la implementación de infraestructuras, servicios y aplicaciones.

Una pila puede configurar la creación automática de la mayoría de los recursos de OpenStack, incluidos instancias, direcciones IP flotantes, volúmenes, grupos de seguridad y usuarios. Para crear una pila, utilice una plantilla de orquestación que defina los parámetros para automatizar la implementación de infraestructuras, servicios y aplicaciones.

También se puede crear una pila en la que se combine una plantilla de orquestación con un archivo de entorno. Un archivo de entorno proporciona un conjunto exclusivo de valores para los parámetros que se definen en la plantilla. Cuando se utilizan archivos de entorno con plantillas, es posible crear muchas pilas exclusivas a partir de una sola plantilla.

VMware Integrated OpenStack admite el formato Heat Orchestration Template (HOT) de OpenStack a través de una API de REST y el formato de plantilla CloudFormation de Amazon Web Services (AWS) a través de una API de consulta que sea compatible con CloudFormation.

Para obtener información sobre cómo crear archivos de plantilla y de entorno para las pilas de Heat, consulte Guía de plantillas en la documentación de OpenStack.

Este capítulo incluye los siguientes temas:

Generar una plantilla de Heat

Puede utilizar el generador de plantillas para crear plantillas de orquestación a través de una interfaz con sistema de arrastrar y soltar.

Se admiten los siguientes tipos de recursos:

- `OS::Cinder::Volume`
- `OS::Cinder::VolumeAttachment`
- `OS::Designate::RecordSet`

- `OS::Designate::Zone`
- `OS::Heat::AutoScalingGroup`
- `OS::Heat::ResourceGroup`
- `OS::Heat::ScalingPolicy`
- `OS::Neutron::FloatingIP`
- `OS::Neutron::FloatingIPAssociation`
- `OS::Neutron::Net`
- `OS::Neutron::Port`
- `OS::Neutron::Router`
- `OS::Neutron::RouterInterface`
- `OS::Neutron::SecurityGroup`
- `OS::Neutron::Subnet`
- `OS::Nova::KeyPair`
- `OS::Nova::Server`
- `OS::Swift::Container`

Procedimiento

1. Inicie sesión en el panel de control de VMware Integrated OpenStack.
2. En el menú desplegable de la barra de título, seleccione el proyecto.
3. Seleccione **Proyecto > Orquestación > Generador de plantillas**.
4. En el menú desplegable **Versión de plantilla**, seleccione la versión de Heat que desee.
5. Arrastre los iconos de los tipos de recursos deseados al lienzo.
6. Haga clic en cada icono para establecer parámetros y dependencias, y haga clic en **Guardar**.
7. Cuando haya agregado y configurado todos los recursos deseados, haga clic en el icono del **generador de plantillas**.
8. Revise la configuración y haga clic en **Descargar** para descargar la plantilla generada o en **Crear pila** para iniciar una pila mediante la plantilla generada.

Iniciar una pila

Con las pilas de orquestación, es posible iniciar y administrar varias aplicaciones compuestas en la nube.

Requisitos previos

Cree la plantilla de orquestación para la pila. Para obtener más información, consulte Guía de plantillas en la documentación de OpenStack.

Procedimiento

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

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

3 Seleccione **Proyecto > Orquestación > Pilas**.

4 Haga clic en **Iniciar pila** e introduzca la plantilla de orquestación.

Opción	Descripción
Origen de la plantilla	Seleccione **archivo**, **Entrada directa** o **Dirección URL**. ■ Si selecciona **Archivo**, haga clic en **Elegir archivo** y cargue la plantilla de orquestación. ■ Si selecciona **Entrada directa**, introduzca la plantilla de orquestación en el campo **Datos de la plantilla**. ■ Si selecciona **Dirección URL**, introduzca la dirección URL en la que se encuentra la plantilla de orquestación.
Origen del entorno	Seleccione **Archivo** o **Entrada directa**. ■ Si selecciona **Archivo**, haga clic en **Elegir archivo** y cargue el archivo de entorno. ■ Si selecciona **Entrada directa**, introduzca el archivo de entorno en el campo **Datos de entorno**.

5 Haga clic en **Siguiente** e introduzca la configuración de la pila.

Opción	Descripción
Nombre de la pila	Introduzca un nombre para la pila.
Tiempo de espera de la creación (minutos)	Introduzca el tiempo en minutos después del cual se agotará el tiempo de creación de la pila.
Reversión en caso de errores	Seleccione la casilla de verificación para revertir los cambios si se producen errores al iniciar la pila.
Contraseña para el usuario "admin"	Introduzca la contraseña del usuario `admin`. Esta contraseña es necesaria para realizar operaciones de orquestación.

6 Haga clic en **Iniciar**.

Pasos siguientes

En la columna **Acciones**, puede suspender, reanudar o eliminar la pila. También puede validar la pila o cambiar su plantilla de orquestación y archivo de entorno.

Parámetros configurables de Heat

Puede modificar ciertos parámetros de la configuración de Heat mediante el uso de `viocli update heat` o la utilidad de línea de comandos `kubectl` de Kubernetes.

Ejemplo de configuración que utiliza `viocli update heat`.

```
conf:
  heat:
    DEFAULT:
      max_stacks_per_tenant: 150
      max_interface_check_attempts: 220
```

Ejemplo de configuración que utiliza `kubectl`.

```
kubectl –n openstack patch heat heat1 ––type=merge ––patch '{"spec":{"conf":{"heat":{"DEFAULT":
{"max_interface_check_attempts":220}}}}}
```

Tabla 8-1. Parámetros de Heat

Parámetro	Valor predeterminado	Descripción
`cron_purge_enabled`	`true`	Introduzca `true` para limpiar automáticamente la base de datos de Heat o introduzca `false` para deshabilitar esta función.
`purge_age_type`	`days`	
`purge_age`	`7`	
`purge_cron_time`	`"1 0 * * *"`	
`max_resources_per_stack`	`1000`	Introduzca la cantidad máxima de recursos que puede usar una pila de Heat.
`max_stacks_per_tenant`	`100`	Introduzca la cantidad máxima de pilas de Heat que puede crear cada proyecto.
`event_purge_batch_size`	`200`	
`max_events_per_stack`	`1000`	
`encrypt_parameters_and_properties`	`false`	
`max_nested_stack_depth`	`5`	
`max_interface_check_attempts`	`60`	
`convergence_engine`	`true`	Introduzca `true` para habilitar el motor de convergencia de Heat o introduzca `false` para deshabilitar esta función.
`observe_on_update`	`false`	
`max_template_size`	`524288`	Introduzca el tamaño de archivo máximo (en bytes) de una plantilla de Heat.

Tabla 8-1. Parámetros de Heat (continuación)

Parámetro	Valor predeterminado	Descripción
stack_action_timeout	3600	Introduzca el tiempo de espera (en segundos) para las acciones de pila de Heat.
max_pool_size	5	Introduzca la cantidad máxima de conexiones de SQL que pueden mantenerse abiertas en un grupo. Si introduce 0, no se limitará el número de conexiones abiertas.
max_overflow	50	
rpc_response_timeout		Introduzca el tiempo (en segundos) que se debe esperar para recibir una respuesta de una instancia de RPC.

Almacenamiento de objetos en Swift

9

Swift es un componente de OpenStack que proporciona almacenamiento de objetos distribuidos.

Importante En VMware Integrated OpenStack 6.0, Swift se proporciona solo como una vista previa técnica. Actualmente no se admite la ejecución de cargas de trabajo de producción.

Para obtener más información sobre Swift, consulte la Documentación de OpenStack Swift.

Este capítulo incluye los siguientes temas:

- Crear el clúster de Swift
- Agregar nodos al clúster de Swift
- Almacenar objetos en Swift

Crear el clúster de Swift

La creación del clúster de Swift inicia los servicios de Swift y genera los nodos necesarios.

Importante En VMware Integrated OpenStack 6.0, Swift se proporciona solo como una vista previa técnica. Actualmente no se admite la ejecución de cargas de trabajo de producción.

Requisitos previos

- Asegúrese de que haya suficientes recursos disponibles para implementar Swift. Los recursos necesarios dependen de la escala de la implementación.
- Asegúrese de que todos los hosts del clúster de Swift utilizan un almacén de datos compartido (vSAN o NFS). Los almacenes de datos locales no son compatibles con Swift.
- Compruebe que todos los almacenes de datos incluidos en el clúster de Swift estén disponibles para todos los nodos de controlador de la implementación.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 En un editor de texto, cree el archivo de configuración para el clúster de Swift en formato YAML.

El archivo de configuración debe definir tres nodos Swift. Utilice la siguiente plantilla:

```
---
nodes:
- datastore: node1-datastore
  disk_size: node1-disksize-GB
  name: node1-name
  zone: node1-zone
- datastore: node2-datastore
  disk_size: node2-disksize-GB
  name: node2-name
  zone: node2-zone
- datastore: node3-datastore
  disk_size: node3-disksize-GB
  name: node3-name
  zone: node3-zone
```

Opción	Descripción
node-datastore	Introduzca el nombre del almacén de datos para el nodo Swift especificado.
node-disksize-GB	Introduzca el tamaño de disco deseado en gigabytes.
node-name	Introduzca un nombre para el nodo Swift especificado. El nombre de cada nodo debe ser único.
node-zone	Introduzca el número de zona Swift del nodo Swift especificado. El número de zona debe ser un número entero.

3 Cree el clúster de Swift mediante el archivo de configuración definido en el paso anterior.

```
viocli create swift -f swift-config-file
```

Resultados

Se crean los pods que se requieren para el clúster de Swift y se habilita el servicio.

Pasos siguientes

Para escalar horizontalmente el clúster, consulte Agregar nodos al clúster de Swift.

Para eliminar el clúster de Swift, ejecute el comando `viocli delete swift`.

Agregar nodos al clúster de Swift

Puede agregar nodos para escalar horizontalmente el clúster de Swift.

Importante En VMware Integrated OpenStack 6.0, Swift se proporciona solo como una vista previa técnica. Actualmente no se admite la ejecución de cargas de trabajo de producción.

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.

Requisitos previos

Implementar Swift. Consulte Crear el clúster de Swift.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Agregue un nodo al clúster.

```
viocli add swiftnode --name node-name --datastore node-datastore --zone node-zone --disk-size
node-disksize-gb
```

Opción	Descripción
node-name	Introduzca un nombre para el nodo Swift. El nombre de cada nodo debe ser único.
node-datastore	Introduzca el nombre del almacén de datos del nodo. Solo se admiten almacenes de datos compartidos (vSAN o NFS). Los nodos Swift no se pueden crear en almacenes de datos locales.
node-zone	Introduzca el número de zona Swift del nodo. El número de zona debe ser un número entero.
node-disksize-gb	Introduzca el tamaño de disco deseado en gigabytes.

Almacenar objetos en Swift

Puede crear contenedores en Swift y cargar objetos en ellos.

Importante En VMware Integrated OpenStack 6.0, Swift se proporciona solo como una vista previa técnica. Actualmente no se admite la ejecución de cargas de trabajo de producción.

Requisitos previos

Implementar Swift. Consulte Crear el clúster de Swift.

Procedimiento

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

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

3 Seleccione **Proyecto > Almacén de objetos > Contenedores** y haga clic en **Contenedor**.

4 Introduzca un nombre y haga clic en **Enviar**.

El nombre de un contenedor no puede incluir barras diagonales (/).

5 Haga clic en el nombre del contenedor para abrirlo.

6 (opcional) Haga clic en el botón **Carpeta** para crear una carpeta.

7 Haga clic en el botón **Cargar** (flecha hacia arriba) para cargar un archivo en el contenedor.

Pasos siguientes

Puede descargar o eliminar archivos del contenedor. También puede hacer clic en la flecha hacia abajo junto a cualquier archivo para ver sus detalles o seleccionar **Editar** para reemplazarlo por otro archivo.

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
- Crear una tarea de copia de seguridad programada
- Configurar el servicio de copia de seguridad para Cinder
- Restaurar la implementación desde una copia de seguridad

Hacer una copia de seguridad de la implementación

Puede usar la línea de comandos para realizar una copia de seguridad de la implementación de OpenStack.

Importante El archivo de configuración temporal que se creó en este procedimiento contiene las credenciales de vCenter Server en texto no cifrado. Por motivos de seguridad, elimine este archivo tras finalizar la creación de la copia de seguridad.

Se creó una copia de seguridad de los siguientes elementos:

- Configuraciones de los componentes de OpenStack
- Base de datos del plano de control de OpenStack
- Secretos de implementación

Para obtener información sobre la creación de copias de seguridad de Cinder, consulte Configurar el servicio de copia de seguridad para Cinder.

Requisitos previos

Cree una biblioteca de contenido en la instancia de vCenter Server. Para obtener información sobre bibliotecas de contenido, consulte Usar bibliotecas de contenido.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 En un editor de texto, cree el archivo de configuración para la copia de seguridad en formato YAML.

Utilice la siguiente plantilla:

```
---
name: backup-name
description: backup-description
target:
   kind: contentLibrary
   contentLibrary:
      name: content-library-name
      hostname: vcserver-fqdn
      username: vcserver-admin
      password: vcserver-password
```

Opción	Descripción
backup-name	Introduzca un nombre para la copia de seguridad. La cadena alfanumérica puede incluir caracteres especiales (-) y (_).
backup-description	Introduzca una descripción de la copia de seguridad.
content-library-name	Introduzca el nombre de la biblioteca de contenido para el archivo guardado de copia de seguridad.
vcserver-fqdn	Introduzca el FQDN de la instancia de vCenter Server que contiene la biblioteca de contenido.
vcserver-admin	Introduzca el nombre de usuario de un administrador de vCenter Server.
vcserver-password	Introduzca la contraseña del administrador de vCenter Server especificado.

3 Cree la copia de seguridad con el archivo de configuración.

```
viocli create backup -f <configuration-file>
```

Resultados

Se guarda una copia de seguridad de la implementación en la biblioteca de contenido que especificó en el archivo de configuración de copia de seguridad.

Crear una tarea de copia de seguridad programada

Puede configurar la implementación para que se realice una copia de seguridad automática según una programación regular.

Importante El archivo de configuración temporal que se creó en este procedimiento contiene las credenciales de vCenter Server en texto no cifrado. Por motivos de seguridad, elimine este archivo tras crear la tarea de copia de seguridad.

Se creó una copia de seguridad de los siguientes elementos:

- Configuraciones de los componentes de OpenStack
- Base de datos del plano de control de OpenStack
- Secretos de implementación

Para obtener información sobre la creación de copias de seguridad de Cinder, consulte Configurar el servicio de copia de seguridad para Cinder.

Requisitos previos

Cree una biblioteca de contenido en la instancia de vCenter Server. Para obtener información sobre bibliotecas de contenido, consulte Usar bibliotecas de contenido.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 En un editor de texto, cree el archivo de configuración para la copia de seguridad programada en formato YAML.

Utilice la siguiente plantilla:

```
---
namePrefix: backup-name-prefix
description: backup-description
backupSchedule: backup-schedule
retentionPolicy:
  maximumNumberOfBackup: max-backups
target:
   kind: contentLibrary
   contentLibrary:
```

```
      name: content-library-name
      hostname: vcserver-fqdn
      username: vcserver-admin
      password: vcserver-password
```

Opción	Descripción
backup-name-prefix	Introduzca un prefijo para los archivos de copia de seguridad. La cadena alfanumérica puede incluir el carácter especial (-).
backup-description	Introduzca una descripción de la copia de seguridad.
backup-schedule	Especifique la programación de copia de seguridad como una expresión cron de cinco campos. Por ejemplo, introduzca **"5 0 * * *"** para realizar una copia de seguridad todos los días a las 00:05.
max-backups	El número máximo de copias de seguridad que se conservarán. Introduzca un número entero superior a 0.
content-library-name	Introduzca el nombre de la biblioteca de contenido para el archivo guardado de copia de seguridad.
vcserver-fqdn	Introduzca el FQDN de la instancia de vCenter Server que contiene la biblioteca de contenido.
vcserver-admin	Introduzca el nombre de usuario de un administrador de vCenter Server.
vcserver-password	Introduzca la contraseña del administrador de vCenter Server especificado.

3 Cree la tarea de copia de seguridad con el archivo de configuración.

```
viocli create backupschedule –f <configuration-file>
```

Resultados

Se crea la tarea de copia de seguridad y las copias de seguridad de la implementación se guardan en la biblioteca de contenido de acuerdo con la programación especificada.

Configurar el servicio de copia de seguridad para Cinder

Puede configurar Cinder para realizar copias de seguridad de volúmenes en un servidor de Network File System (NFS).

Requisitos previos

- Cree un directorio NFS compartido dedicado al almacenamiento de copias de seguridad de Cinder.
- Compruebe que el usuario de `root` (UID 0) sea el propietario de la carpeta compartida de NFS.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Edite la configuración de Cinder.

```
viocli update cinder
```

3 En la sección `conf`, cree la sección `cinder`. En la sección `cinder`, cree la sección `DEFAULT`.

4 En la sección `DEFAULT`, agregue el parámetro `backup_driver` y establezca el valor como `cinder.backup.drivers.nfs.NFSBackupDriver`.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  backends:
    [...]
  cinder:
    DEFAULT:
      backup_driver: cinder.backup.drivers.nfs.NFSBackupDriver
```

5 Agregue el parámetro `backup_mount_options` y establezca el valor como la versión de NFS que posee.

Por ejemplo, introduzca **`vers=4`** para admitir la versión 4 de NFS.

6 Agregue el parámetro `backup_share` y establezca el valor como la ubicación del directorio NFS compartido.

Use el formato *nfs-host:path*. Por ejemplo, `192.0.2.100:/cinder`.

7 Cree la sección `manifests`.

8 En la sección `manifests`, agregue el parámetro `deployment_backup` y establezca el valor como **`true`**.

9 Agregue el parámetro `job_backup_storage_init` y establezca el valor como **`true`**.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  backends:
    [...]
  cinder:
    DEFAULT:
      backup_driver: cinder.backup.drivers.nfs.NFSBackupDriver
      backup_mount_options: nfs-version
      backup_share: nfs-host:path
manifests:
  deployment_backup: true
  job_backup_storage_init: true
```

Resultados

Ahora puede usar el comando `cinder backup-create` para realizar una copia de seguridad de los volúmenes de Cinder.

Restaurar la implementación desde una copia de seguridad

Puede restaurar la implementación de VMware Integrated OpenStack a partir de una copia de seguridad.

Importante

- El archivo de configuración temporal que se creó en este procedimiento contiene las credenciales de vCenter Server en texto no cifrado. Por motivos de seguridad, elimine este archivo tras finalizar la creación de la copia de seguridad.
- No realice varias operaciones de restauración al mismo tiempo. Si una operación de restauración no está configurada correctamente, espere hasta que se produzca un error en la operación o se agote el tiempo de espera antes de volver a intentarlo.

Requisitos previos

Compruebe que haya una copia de seguridad disponible. Consulte Hacer una copia de seguridad de la implementación o Crear una tarea de copia de seguridad programada.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 En un editor de texto, cree el archivo de configuración de restauración en formato YAML.

- Si desea restaurar la instancia de VMware Integrated OpenStack en un plano de control existente, utilice la siguiente plantilla:

```
---
name: backup-file-name
description: restore-description
source:
   kind: contentLibrary
   contentLibrary:
      name: content-library-name
      hostname: content-library-vcserver-fqdn
      username: content-library-vcserver-admin
      password: content-library-vcserver-password
datastore: control-plane-storage
```

A continuación se describen los parámetros.

Opción	Descripción
backup-file-name	Introduzca el nombre del archivo de copia de seguridad para restaurar.
restore-description	Introduzca una descripción para la tarea de restauración.
content-library-name	Introduzca el nombre de la biblioteca de contenido que contiene el archivo de copia de seguridad.
content-library-vcserver-fqdn	Introduzca el FQDN de la instancia de vCenter Server que contiene la biblioteca de contenido.
content-library-vcserver-admin	Introduzca el nombre de usuario de un administrador de vCenter Server en esa instancia.
content-library-vcserver-password	Introduzca la contraseña del administrador de vCenter Server especificado.
control-plane-storage	(Opcional) Introduzca el nombre del almacén de datos en el que se almacenará la información del plano de control.

- Si desea restaurar la instancia de VMware Integrated OpenStack en un nuevo plano de control, utilice la siguiente plantilla:

```
---
hostname: vio-vcserver-fqdn
username: vio-vcserver-admin
password: vio-vcserver-password
---
cluster:
  network_info:
  - networkName: mgmt-network-name
    type: management
    static_config:
      ip_ranges:
      - mgmt-ip-range-begin, mgmt-ip-range-end
      netmask: mgmt-subnet-mask
      gateway: mgmt-gateway-address
      dns:
      - mgmt-dns-server
  - networkName: api-network-name
    type: api
    static_config:
      ip_ranges:
      - api-ip-range-begin, api-ip-range-end
      netmask: api-subnet-mask
      gateway: api-gateway-address
      dns:
      - api-dns-server
  - networkName: trunk-network-name
    type: dvs_trunk_network
    static_config:
      ip_ranges:
```

```
      - trunk-ip-range-begin, trunk-ip-range-end
---
datacenter: datacenter-name
datastore: datastore-name
resourcePool: resource-pool-name
count: controller-count
size: controller-size
---
name: backup-file-name
description: restore-description
source:
   kind: contentLibrary
   contentLibrary:
      name: content-library-name
      hostname: content-library-vcserver-fqdn
      username: content-library-vcserver-admin
      password: content-library-vcserver-password
datastore: control-plane-storage
```

A continuación se describen los parámetros.

Tabla 10-1. Configuración de vCenter Server

Opción	Descripción
vio-vcserver-fqdn	Introduzca el FQDN de la instancia de vCenter Server en la que desea restaurar la implementación.
vio-vcserver-admin	Introduzca el nombre de usuario de un administrador de vCenter Server en esa instancia.
vio-vcserver-password	Introduzca la contraseña del administrador de vCenter Server especificado.

Tabla 10-2. Configuración de red de administración

Opción	Descripción
mgmt-network-name	Introduzca el nombre de la red de administración.

Si la red de administración utiliza direcciones IP estáticas en lugar de DHCP, introduzca los siguientes valores. Estos valores no son necesarios para redes DHCP.

Opción	Descripción
mgmt-ip-range-begin, *mgmt-ip-range-end*	Introduzca los rangos de direcciones IP en la red de administración en formato decimal con puntos, separados por comas. Por ejemplo, **192.0.2.10, 192.0.2.50**.
mgmt-subnet-mask	Introduzca la máscara de subred de la red de administración.

Opción	Descripción
mgmt-gateway-address	Introduzca la dirección IP de la puerta de enlace de red para la red de administración.
mgmt-dns-server	Introduzca la dirección IP de uno o varios servidores DNS para la red de administración. Introduzca cada dirección IP en una línea independiente. Por ejemplo: – `192.0.2.1` – `192.0.2.100`

Tabla 10-3. Configuración de red de acceso a API

Opción	Descripción
api-network-name	Introduzca el nombre de la red de acceso a la API.

Si la red de acceso a la API utiliza direcciones IP estáticas en lugar de DHCP, introduzca los siguientes valores. Estos valores no son necesarios para redes DHCP.

Opción	Descripción
api-ip-range-begin, *api-ip-range-end*	Introduzca los rangos de direcciones IP en la red de acceso a la API en formato decimal con puntos, separados por comas. Por ejemplo, **`198.51.100.10, 198.51.100.50`**.
api-subnet-mask	Introduzca la máscara de subred para la red de acceso a la API.
api-gateway-address	Introduzca la dirección IP de la puerta de enlace de red para la red de acceso a la API.
api-dns-server	Introduzca la dirección IP de uno o varios servidores DNS para la red de acceso a la API. Introduzca cada dirección IP en una línea independiente. Por ejemplo: – `198.51.100.1` – `198.51.100.100`

Si la implementación usa redes de VDS, introduzca los siguientes valores. Estos valores no son necesario para las implementaciones de NSX.

Tabla 10-4. Configuración de red troncal

Opción	Descripción
trunk-network-name	Introduzca el nombre de la red troncal.
trunk-ip-range-begin, *trunk-ip-range-end*	Introduzca los rangos de direcciones IP en la red troncal en formato decimal con puntos, separados por comas. Por ejemplo, **`169.254.0.1,169.254.0.254`**.

Introduzca la siguiente información para todos los tipos de implementación.

Tabla 10-5. Configuración de plano de control

Opción	Descripción
datacenter-name	Introduzca el nombre del centro de datos de vSphere en el que se creará el plano de control de VMware Integrated OpenStack.
datastore-name	Introduzca el nombre del almacén de datos para el plano de control de VMware Integrated OpenStack.
resource-pool-name	Introduzca el nombre del grupo de recursos para el plano de control de VMware Integrated OpenStack.
controller-count	Especifique la cantidad de controladores que se crearán.
controller-size	Especifique el tamaño de los controladores. Se aceptan los siguientes valores: ■ **`small`** (4 vCPU y 16 GB de RAM) ■ **`medium`** (8 vCPU y 32 GB de RAM) ■ **`large`** (12 vCPU y 32 GB de RAM)

Tabla 10-6. Configuración de copia de seguridad

Opción	Descripción
backup-file-name	Introduzca el nombre del archivo de copia de seguridad para restaurar.
restore-description	Introduzca una descripción para la tarea de restauración.
content-library-name	Introduzca el nombre de la biblioteca de contenido que contiene el archivo de copia de seguridad.

Si la biblioteca de contenido y la instancia de VMware Integrated OpenStack se encuentran en instancias de vCenter Server separadas, introduzca la configuración de la instancia de vCenter Server que contiene la biblioteca de contenido. Los siguientes valores no son necesarios si la biblioteca de contenido y el plano de control se encuentran en la misma instancia de vCenter Server.

Tabla 10-7. Configuración de biblioteca de contenido

Opción	Descripción
content-library-vcserver-fqdn	Introduzca el FQDN de la instancia de vCenter Server que contiene la biblioteca de contenido.
content-library-vcserver-admin	Introduzca el nombre de usuario de un administrador de vCenter Server en esa instancia.

Tabla 10-7. Configuración de biblioteca de contenido (continuación)

Opción	Descripción
content-library-vcserver-password	Introduzca la contraseña del administrador de vCenter Server especificado.
control-plane-storage	(Opcional) Introduzca el nombre del almacén de datos en el que se almacenará la información del plano de control.

3 Ejecute el comando `viocli restore deployment` y especifique el archivo de configuración de restauración.

```
viocli restore deployment –f configuration–file [––skip–control–plane]
```

Para restaurar la implementación en un plano de control existente, incluya el parámetro `––skip–control–plane`.

Resultados

La implementación de OpenStack se restaura al estado que tenía en la copia de seguridad.

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:

Crear un paquete de soporte

Puede crear un paquete de soporte que incluya registros de la implementación de VMware Integrated OpenStack a modo de ayuda en la solución de problemas.

Procedimiento

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Cree un paquete de soporte.

```
viocli generate supportbundle
```

Resultados

Los archivos de registro se recopilan en un paquete de soporte. Puede utilizarlo para solucionar problemas o proporcionarlo al personal de asistencia técnica cuando solicite asistencia.

Error al implementar un dispositivo virtual de VMware Integrated OpenStack

Al instalar el archivo OVA de VMware Integrated OpenStack, recibe el mensaje de error `The operation is not supported on the object.`

Causa

Este error se produce cuando DRS está deshabilitado en el clúster de administración donde se instala el archivo OVA de VMware Integrated OpenStack.

Solución

1. En vSphere Client, seleccione el clúster de administración.
2. En la pestaña **Configurar**, seleccione **Servicios > vSphere DRS**.
3. Haga clic en **Editar** y habilite **vSphere DRS**.

Sincronizar el estado de la instancia de OpenStack

Es posible restablecer las instancias de OpenStack con el estado `SHUTOFF` o `ERROR` que se encuentran encendidas en vCenter Server.

Problema

Una instancia de OpenStack puede permanecer en el estado `ERROR` o `SHUTOFF` incluso después de que la máquina virtual correspondiente a la instancia se enciende en vCenter Server.

Solución

1. Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

   ```
   ssh root@mgmt-server-ip
   ```

2. Consulte las instancias de OpenStack en el estado `ERROR` o `SHUTOFF` que se muestran como encendidas en vCenter Server.

   ```
   viocli get instances --nova-state {ERROR | SHUTOFF} --vc-state poweredOn
   ```

3. Restablezca las instancias encendidas en el estado `ERROR` o `SHUTOFF`.

   ```
   viocli reset instances --nova-state {ERROR | SHUTOFF}
   ```

La tabla de instancias de proyecto tarda en aparecer

En entornos de gran escala, el panel de control de VMware Integrated OpenStack puede tardar en mostrar la tabla de instancias de un proyecto de OpenStack.

Problema

Cuando se inicia sesión en el panel de control de VMware Integrated OpenStack y se selecciona **Proyecto > Proceso > Instancias**, el panel de control tarda más de lo esperado en mostrar la lista de instancias.

Para solucionar este problema, puede configurar el panel de control a fin de obtener la información de la dirección IP de Nova en lugar de Neutron. Aunque esto mejora el rendimiento de la página de la instancia, es posible que la información de la dirección IP en esa página no se muestre inmediatamente.

Solución

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Modifique la configuración de Horizon.

```
viocli update horizon
```

3 En la sección `config`, agregue el parámetro `horizon_instance_retrieve_ip_address` y establezca el valor como `false`.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  horizon:
    local_settings:
      config:
        horizon_instance_retrieve_ip_address: false
        openstack_neutron_network:
          neutron_backend: network-mode
```

Error intermitente en la eliminación de usuarios

En escenarios de alta concurrencia, es posible que se produzcan errores intermitentes al eliminar usuarios de OpenStack.

Problema

Cuando se intenta eliminar un usuario de OpenStack, aparece este mensaje de error:

```
Failed to consume a task from the queue: Gateway Timeout (HTTP 504): GatewayTimeout: Gateway Timeout
(HTTP 504)
```

Para solucionar este problema, modifique el tiempo de espera de bloqueo de espera de la base de datos.

Solución

1 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

2 Modifique la configuración de MariaDB.

```
viocli update mariadb
```

3 En la sección `conf`, agregue el parámetro `innodb_lock_wait_timeout` y establezca el valor como `1000`.

El archivo de configuración incluye:

```
conf:
  innodb_lock_wait_timeout: 1000
```

Se produce un error en la copia de seguridad de Cinder con alta concurrencia

La configuración predeterminada de VMware Integrated OpenStack puede ser insuficiente para las operaciones de copia de seguridad de Cinder con grandes volúmenes o alta concurrencia.

Problema

Cuando se aumenta la concurrencia de las operaciones de copia de seguridad de Cinder o el tamaño de los volúmenes de Cinder, es posible que se produzca un error en las operaciones y que se muestren errores de `GetResourceFailure` en los registros.

Solución

1 Escale horizontalmente el plano de control y la cantidad de pods de copia de seguridad de Cinder.

Cada nodo de controladora puede contener un solo pod de copia de seguridad de Cinder.

a Aumente la cantidad de nodos de controladora en la implementación.

Consulte Add Controller Nodes to Your Deployment.

b Aumente la cantidad de pods de copia de seguridad de Cinder en la implementación.

Consulte Escalar servicios de OpenStack.

2 Inicie sesión en Integrated OpenStack Manager como el usuario de `root`.

```
ssh root@mgmt-server-ip
```

3 Actualice el tamaño del grupo de subprocesos del ejecutor y el tiempo de espera de respuesta de RPC para Cinder.

   a Modifique la configuración de Cinder.

   ```
   viocli update cinder
   ```

   b En la sección `DEFAULT`, agregue el parámetro `rpc_response_timeout` y establezca el valor como `6000`.

   c Agregue el parámetro `executor_thread_pool_size` y establezca el valor en `640`.

   El archivo de configuración ahora tiene un aspecto similar al siguiente:

   ```
   conf:
     backends:
       [...]
     cinder:
       DEFAULT:
         [...]
         rpc_response_timeout: 6000
         executor_thread_pool_size: 640
   ```

4 Actualice el tiempo de espera de la base de datos y los parámetros de conexión máximos.

   a Modifique la configuración de MariaDB.

   ```
   viocli update mariadb
   ```

   b En la sección `conf`, agregue el parámetro `connect_timeout` y establezca el valor como `5`.

   c Agregue el parámetro `max_connections` y establezca el valor en `5000`.

   d Agregue el parámetro `net_read_timeout` y establezca el valor en `1200`.

   e Agregue el parámetro `net_write_timeout` y establezca el valor en `1200`.

   f En la sección `conf`, agregue la sección `ingress`.

   g En la sección `ingress`, agregue el parámetro `proxy-read-timeout` y establezca el valor como `1200`.

h Agregue el parámetro `proxy-send-timeout` y establezca el valor en `1200`.

i Agregue el parámetro `proxy-stream-timeout` y establezca el valor en `3600s`.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  connect_timeout: 5
  max_connections: 5000
  net_read_timeout: 1200
  net_write_timeout: 1200
  ingress:
    proxy-read-timeout: 1200
    proxy-send-timeout: 1200
    proxy-stream-timeout: 3600s
```

5 Actualice los tamaños de grupo y los índices de asignación de Nova.

a Modifique la configuración de Nova.

```
viocli update nova
```

b En la sección `nova`, agregue la sección `DEFAULT`.

c En la sección `DEFAULT`, agregue el parámetro `cpu_allocation_ratio` y establezca el valor como `30`.

d Agregue el parámetro `executor_thread_pool_size` y establezca el valor en `640`.

e Agregue el parámetro `ram_allocation_ratio` y establezca el valor en `6`.

f En la sección `nova`, agregue la sección `database`.

g En la sección `database`, agregue el parámetro `max_pool_size` y establezca el valor como `50`.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  nova:
    DEFAULT:
      cpu_allocation_ratio: 30
      executor_thread_pool_size: 640
      ram_allocation_ratio: 6
    database:
      max_pool_size: 50
```

6 Actualice los parámetros de caducidad del token y de la interfaz de puerta de enlace de servidor web (Web Server Gateway Interface, WSGI) de Keystone.

a Modifique la configuración de Keystone.

```
viocli update keystone
```

b En la sección `conf`, agregue la sección `keystone`.

c En la sección `keystone`, agregue el parámetro `wsgi_processes` y establezca el valor como `8`.

d Agregue el parámetro `wsgi_threads` y establezca el valor en `15`.

e En la sección `keystone`, agregue la sección `token`.

f En la sección `token`, agregue el parámetro `expiration` y establezca el valor como `28800`.

El archivo de configuración ahora tiene un aspecto similar al siguiente:

```
conf:
  keystone:
    wsgi_processes: 8
    wsgi_threads: 15
      token:
        expiration: 28800
```

VMware Integrated OpenStack Command Reference

12

VMware Integrated OpenStack includes the `viocli` utility to configure and manage your deployment on the command line. To use `viocli`, connect to the Integrated OpenStack Manager over SSH and log in as the `root` user.

For NSX deployments, the `nsxadmin` utility is also provided to perform certain network-related operations. You must log in to a Neutron server pod to use `nsxadmin`. For information about `nsxadmin` commands, see the Documentación de nsxadmin.

The Kubernetes `kubectl` command-line utility may be required for some operations. For more information about `kubectl`, see the official Kubernetes documentation.

The following aliases are provided to improve user experience for operators.

Alias	Kubectl Command
`osctl`	`kubectl –n openstack`
`osapply`	`kubectl –n openstack apply`
`osctlw`	`kubectl –n openstack ––watch`
`osdel`	`kubectl –n openstack delete`
`osedit`	`kubectl –n openstack edit`
`osget`	`kubectl –n openstack get`
`oslog`	`kubectl –n openstack logs`

In addition, the `viossh` *`controller–node–name`* alias allows you to log in to a controller node.

Este capítulo incluye los siguientes temas:

- Comparación de operaciones de la línea de comandos
- Cuadro de herramientas de VMware Integrated OpenStack
- Comando viocli add
- Comando viocli create
- Comando viocli delete
- Comando viocli generate

Comparación de operaciones de la línea de comandos

En VMware Integrated OpenStack 6.0, se refactorizaron utilidades de la línea de comandos. En la siguiente tabla, se enumeran las operaciones de la línea de comandos en VMware Integrated OpenStack 5.1 y sus equivalentes en la versión 6.0.

Tabla 12-1. Comparación de operaciones de la línea de comandos

Comando de VMware Integrated OpenStack 5.1	Comando de VMware Integrated OpenStack 6.0
`viocli backup`	`viocli create backup`
`viocli barbican`	Este comando está obsoleto. Utilice la interfaz web de Integrated OpenStack Manager para configurar Barbican.
`viocli certificate add`	`viocli import certificate`
`viocli certificate list`	`viocli get certificates`
`viocli certificate remove`	Este comando está obsoleto. Utilice el comando `viocli import certificate` para reemplazar certificados incorrectos o caducados.
`viocli certificate show`	`viocli get certificates`
`viocli dbverify`	Este comando está obsoleto.
`viocli deployment cert-req-create`	`viocli create csr`
`viocli deployment cert-update`	`viocli import certificate`
`viocli deployment configure`	Este comando está obsoleto. Cuando se utiliza el comando `viocli update` para configurar la implementación, los cambios se aplican inmediatamente.
`viocli deployment default`	Este comando está obsoleto.
`viocli deployment getlogs`	`viocli generate supportbundle`
`viocli deployment pause`	Este comando está obsoleto.
`viocli deployment post-deploy`	Este comando está obsoleto.

Tabla 12-1. Comparación de operaciones de la línea de comandos (continuación)

Comando de VMware Integrated OpenStack 5.1	Comando de VMware Integrated OpenStack 6.0
`viocli deployment reset_status`	Este comando está obsoleto.
`viocli deployment resume`	Este comando está obsoleto.
`viocli deployment run-custom-playbook`	Este comando está obsoleto.
`viocli deployment start`	Este comando está obsoleto.
`viocli deployment status`	`viocli get deployment`
`viocli deployment stop`	Este comando está obsoleto.
`viocli ds-migrate-prep`	`viocli prepare datastore`
`viocli enable-tvd`	`viocli add tvd`
`viocli epops`	Este comando está obsoleto. Los agentes de End Point Operations Management ya no se utilizan para la integración con vRealize Operations Manager.
`viocli federation`	Este comando está obsoleto. Utilice la interfaz web de Integrated OpenStack Manager para configurar la federación de identidades.
`viocli identity`	Este comando está obsoleto. Utilice la interfaz web de Integrated OpenStack Manager para configurar la autenticación.
`viocli inventory-admin clean-instance-vms`	`viocli delete orphaned-managed-vms`
`viocli inventory-admin clean-instances`	`viocli delete orphaned-instances`
`viocli inventory-admin clean-shadow-vms`	`viocli delete orphaned-shadow-vms`
`viocli inventory-admin create-tenant-vdc`	`viocli create tenant-vdc`
`viocli inventory-admin delete-tenant-vdc`	`viocli delete tenant-vdc`
`viocli inventory-admin list-tenant-vdcs`	`viocli get tenant-vdcs`
`viocli inventory-admin reset-instances-state`	`viocli reset instances`
`viocli inventory-admin show-availability-zones`	`viocli get availability-zones`
`viocli inventory-admin show-hypervisors`	`viocli get hypervisors`
`viocli inventory-admin show-instance-vms`	`viocli get managed-vms`
`viocli inventory-admin show-instances`	`viocli get instances`
`viocli inventory-admin show-shadow-vms`	`viocli get shadow-vms`
`viocli inventory-admin show-tenant-vdc`	`viocli get tenant-vdcs`
`viocli inventory-admin sync-availability-zones`	Este comando está obsoleto. Ya no es necesario sincronizar las zonas de disponibilidad.
`viocli inventory-admin update-tenant-vdc`	`viocli update tenant-vdc`
`viocli lbaasv2-enable`	Este comando está obsoleto.
`viocli recover`	Este comando está obsoleto. Los nodos se recuperan automáticamente.
`viocli restore`	`viocli restore deployment`

Tabla 12-1. Comparación de operaciones de la línea de comandos (continuación)

Comando de VMware Integrated OpenStack 5.1	Comando de VMware Integrated OpenStack 6.0
`viocli rollback`	Este comando está obsoleto.
`viocli services start`	`viocli start services`
`viocli services stop`	`viocli stop services`
`viocli show`	`viocli get controllers`
`viocli swift add-proxy`	`viocli add swiftnode`
`viocli swift add-storage`	`viocli add swiftnode`
`viocli swift create-cluster`	`viocli create swift`
`viocli swift delete-cluster`	`viocli delete swift`
`viocli swift list-datastore-zone-mapping`	Este comando está obsoleto.
`viocli upgrade`	Este comando está obsoleto.
`viocli volume-migrate`	`viocli migrate volume`
`viocli vros`	Este comando está obsoleto. Ya no se admite la integración con vRealize Automation.
`viopatch add`	Estos comandos son obsoletos. No se admite la aplicación de revisiones en VMware Integrated OpenStack 6.0.
`viopatch install`	
`viopatch list`	
`viopatch snapshot`	
`viopatch uninstall`	
`viopatch version`	`viocli version`

Cuadro de herramientas de VMware Integrated OpenStack

VMware Integrated OpenStack incluye un contenedor del cuadro de herramientas en el que puede ejecutar clientes de la línea de comandos de OpenStack y otras utilidades.

Para acceder al cuadro de herramientas, inicie sesión en Integrated OpenStack Manager como usuario `root` y ejecute el comando `toolbox`.

Cliente de OpenStack

El cuadro de herramientas incluye los siguientes clientes de OpenStack:

- Aodh
- Barbican
- Cinder
- Designate
- Glance

- Gnocchi
- Heat
- Keystone
- Neutron
- Nova
- Swift

El cuadro de herramientas se configura automáticamente con los ajustes del usuario `admin` en la implementación de OpenStack. Para iniciar sesión como otro usuario, descargue el archivo RC desde el panel de control de VMware Integrated OpenStack y aplíquelo al contenedor del cuadro de herramientas.

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

2 En el menú situado en la esquina superior derecha, seleccione **Archivo RC de OpenStack**.

3 Transfiera el archivo al contenedor del cuadro de herramientas de VMware Integrated OpenStack.

4 Para aplicar la configuración, ejecute el comando `source` *`rc-file`*.

Otras utilidades

Además de los clientes de OpenStack, el cuadro de herramientas incluye Data Center Command-Line Interface (DCLI). Para usar DCLI, ejecute el comando `dcli` y especifique el endpoint de OpenStack privado de la implementación.

```
dcli +server http://internal-vip:9449/api +i
```

Si desea obtener más información, consulte la Página de VMware Data Center CLI en VMware {code}.

Nota La utilidad `nsxadmin` no se puede ejecutar desde el cuadro de herramientas. Para utilizar `nsxadmin`, abra un shell en el contenedor del servidor de Neutron:

```
kubectl -n openstack exec -it neutron-server-pod-name -- /bin/bash
```

Comando viocli add

Utilice el comando `viocli add` para agregar complementos y recursos a la implementación de VMware Integrated OpenStack.

El comando `viocli add` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
–v o ––verbose	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli add –h` o `viocli add ––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 add swiftnode –h` muestra los parámetros para la acción `swiftnode`.

A continuación, se enumeran las acciones que admite `viocli add`.

viocli add swiftnode ––name *node–name* ––datastore *ds–name* ––zone *swift–zone* ––disk–size *size–gb* [–v]

Agrega un nodo al clúster de Swift.

Parámetro	Obligatorio u opcional	Descripción
––name *node-name*	Obligatorio	Especifica el nombre del nuevo nodo.
––datastore *ds-name*	Obligatorio	Especifica el almacén de datos en el que se va a crear el nodo.
––zone *swift-zone*	Obligatorio	Especifica la zona de Swift en la que se colocará el nodo.
––disk–size *size-gb*	Obligatorio	Especifica el tamaño de disco en gigabytes para el nodo.

viocli add tvd –m *manager–ip* –u *nsx–username* –p *nsx–password* ––insecure {true | false} ––overlay–tz *overlay–tz* ––vlan–tz *vlan–tz* ––tier–0–router *t0–router* ––dhcp–profile *dhcp–profile* ––md–proxy *md–proxy* ––md–proxy–secret *shared–secret* [–v]

Agrega compatibilidad de redes de NSX-T Data Center a una implementación de VMware Integrated OpenStack que se implementó con NSX Data Center for vSphere.

Parámetro	Obligatorio u opcional	Descripción
–m *manager-ip* o ––manager *manager-ip*	Obligatorio	Dirección IP de la instancia de NSX Manager de la implementación de NSX-T Data Center.
–u *nsx-username* o ––username *nsx-username*	Obligatorio	Nombre de usuario del administrador de NSX Manager.
–p *nsx-password* o ––password *nsx-password*	Obligatorio	Contraseña para el administrador de NSX Manager.
––insecure {true | false}	Opcional	Especifica si se debe comprobar el certificado de NSX Manager. Si no se incluye esta opción, se utiliza `true` de forma predeterminada.

Parámetro	Obligatorio u opcional	Descripción
`--overlay-tz` *overlay-tz*	Obligatorio	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.
`--vlan-tz` *vlan-tz*	Obligatorio	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.
`--tier-0-router` *t0-router*	Obligatorio	Nombre o UUID del enrutador de nivel 0 predeterminado que se emplea para conectarse a enrutadores lógicos de nivel 1 y configurar redes externas.
`--dhcp-profile` *dhcp-profile*	Obligatorio	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.
`--md-proxy` *md-proxy*	Obligatorio	Nombre o UUID del servidor proxy de metadatos utilizado para habilitar el servicio de metadatos nativo. Debe crear el servidor proxy de metadatos en NSX-T Data Center antes de usar el complemento.
`--md-proxy-secret`	Obligatorio	Secreto compartido para solicitudes de proxy de metadatos.

Comando viocli create

Utilice el comando `viocli create` para crear copias de seguridad, copias de seguridad programadas, solicitudes de firma del certificado (Certificate Signing Request, CSR), y clústeres y nodos de Swift.

El comando `viocli create` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-f` *config-file* o `--file` *config-file*	Opcional	Ejecuta el comando mediante un archivo de configuración específico.
`-i` o `--interactive`	Opcional	Abre la plantilla de configuración en un editor de texto para poder introducir la información necesaria de forma interactiva. Después de introducir la información, guarde y salga del editor de texto para ejecutar el comando.
`-o` o `--out`	Opcional	Ejecuta el comando sin solicitar una confirmación.
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli create –h` o `viocli create ––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 create backup –h` muestra los parámetros para la acción `backup`.

A continuación, se enumeran las acciones que admite `viocli create`.

viocli create backup {–f *config–file* | –i | –o} [–t *timeout*] [–v]

Crea una copia de seguridad de la implementación de OpenStack. Los siguientes parámetros adicionales se aplican a la acción `backup`.

Parámetro	Obligatorio u opcional	Descripción
`–t` *timeout* o `––timeout` *timeout*	Opcional	Especifica el tiempo en segundos durante el cual `viocli` mostrará el progreso de la operación de copia de seguridad. Si no incluye este parámetro, se utilizará el valor predeterminado de 1800 segundos.

Para obtener más información, consulte Hacer una copia de seguridad de la implementación.

viocli create backupschedule {–f *config–file* | –i | –o} [–v]

Crea una copia de seguridad programada de la implementación de OpenStack. Para obtener más información, consulte Crear una tarea de copia de seguridad programada.

viocli create csr –c *country–code* –t *state–name* –l *city–name* –o *org–name* –u *org–unit* [–s *service–name*] [–d *output–dir*] [–f *config–file* | –i | –o] [–v]

Crea una solicitud de firma del certificado para enviar a una entidad de certificación. Los siguientes parámetros adicionales se aplican a la acción `csr`.

Parámetro	Obligatorio u opcional	Descripción
`–c` *country-code* o `––countries` *country-code*	Obligatorio	Código ISO de dos letras del país en el que se ubica la organización que solicita el certificado.
`–t` *state-name* o `––states` *state-name*	Obligatorio	Nombre completo de la provincia o el estado.
`–l` *city-name* o `––localities` *city-name*	Obligatorio	Nombre de la ciudad o el pueblo.
`–n` *org-name* u `––org–names` *org-name*	Obligatorio	Nombre legal de la organización.

Parámetro	Obligatorio u opcional	Descripción
–u *org-unit* u ––org–units *org-unit*	Obligatorio	Nombre del departamento o de la unidad organizativa.
–s *service-name* o ––services *service-name*	Opcional	Nombre de uno o más servicios de VMware Integrated OpenStack para los que se generará la CSR. Separe varios nombres con comas (,). Si no incluye este parámetro, se genera una CSR para cada servicio de VMware Integrated OpenStack.
–d *output-dir* u ––output *output-dir*	Opcional	Directorio en el que se guardan las CSR. Si no incluye este parámetro, las CSR se guardan en el directorio `./csr`.

viocli create swift {–f *config–file* | –i | –o} [–v]

Crea un clúster de Swift. Para obtener más información, consulte Agregar el componente Swift.

viocli create tenant–vdc ––compute *compute–node* ––name *vdc–name* ––project–id *project–uuid* [––cpu–reserve *cpu–min*] [––cpu–limit *cpu–max*] [––mem–reserve *memory–min*] [––mem–limit *memory–max*] [–f *config–file* | –i | –o] [–v]

Crea un centro de datos virtual (Virtual Data Center, VDC) de arrendatario con la configuración especificada. Los siguientes parámetros adicionales se aplican a la acción `tenant–vdc`.

Parámetro	Obligatorio u opcional	Descripción
––compute *compute-node*	Obligatorio	Nodo informático en el que se creará el VDC de tenant. Para poder encontrar los nombres de los nodos informáticos, ejecute el comando `openstack compute service list`.
––name *vdc-name*	Obligatorio	Nombre del VDC de arrendatario.
––project–id *project-uuid*	Obligatorio	UUID del proyecto en el que se va a crear el VDC de tenant.
––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.

Parámetro	Obligatorio u opcional	Descripción
`--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.

Comando viocli delete

Utilice el comando `viocli delete` para eliminar recursos de la implementación de VMware Integrated OpenStack.

El comando `viocli delete` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`--force`	Opcional	Ejecuta el comando sin confirmación.
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli delete -h` o `viocli delete --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 delete tenant-vdc -h` muestra los parámetros para la acción `tenant`.

A continuación, se enumeran las acciones que admite `viocli delete`.

`viocli delete orphaned-instances [--no-grace-period] [--force] [-v]`

Elimina instancias huérfanas de OpenStack.

Parámetro	Obligatorio u opcional	Descripción
`--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.

viocli delete orphaned-managed-vms [--no-grace-period] [--force] [-v]

Elimina máquinas virtuales huérfanas administradas por OpenStack.

Parámetro	Obligatorio u opcional	Descripción
`--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.

viocli delete orphaned-shadow-vms [--no-grace-period] [--force] [-v]

Elimina máquinas virtuales de sombra huérfanas.

Parámetro	Obligatorio u opcional	Descripción
`--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.

viocli delete swift [--force] [-v]

Elimina el clúster de Swift.

viocli delete tenant-vdc *tvdc-id* [--compute *compute-node*] [--force] [-v]

Elimina máquinas virtuales de sombra huérfanas.

Parámetro	Obligatorio u opcional	Descripción
tvdc-id	Obligatorio	Identificador del VDC de tenant que se va a eliminar.
`--compute` *compute-node*	Opcional	Nodo informático del que se eliminará el VDC de tenant. Si no incluye este parámetro, el VDC de tenant se eliminará de todos los nodos informáticos.

Comando viocli generate

Utilice el comando `viocli generate` para generar un paquete de soporte para la implementación de VMware Integrated OpenStack.

El comando `viocli generate` usa la siguiente sintaxis.

```
viocli generate supportbundle [--path file-path] [-u] [-v]
```

Parámetro	Obligatorio u opcional	Descripción
`--path` *file-path*	Opcional	Directorio en el que se guarda el paquete de soporte. Si no incluye este parámetro, el paquete de soporte se guarda en el directorio `/var/log`.
`-u` o `--uncompressed`	Opcional	Guarda el paquete de soporte como archivos no comprimidos. Si no incluye este parámetro, el paquete de soporte se guarda como un archivo TAR comprimido.
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli generate -h` o `viocli generate --help` para mostrar los parámetros del comando.

viocli get Command

Use the `viocli get` command to view the resources in your deployment.

The `viocli get` command uses the following syntax.

```
viocli get {resources | resource-type} [resource-name [--history]] [-v]
```

- Use the `viocli get controllers` command to display information about all controllers in your deployment. You can include the `-v` parameter to display the validation results of the control plane.
- Use the `viocli get deployment` command to display detailed information about your deployment, including its overall status, the status of your log analytics integration (if configured), and the status of each node.
- Use the `viocli get resources` command to display a list of all resource types in your deployment.
- Use the `viocli get` *resource-type* command to display all resources of a certain type.
- Use the `viocli get` *resource-type resource-name* command to display information about a specific resource.

The following parameters apply to the `viocli get` command when displaying information about a specific resource.

Parameter	Mandatory or Optional	Description
`--history`	Optional	Displays the configuration changes for the specified resource.
`-v` or `--verbose`	Optional	Displays output in verbose mode.

The following additional parameters apply to the `instances` resource.

Parameter	Mandatory or Optional	Description
`--nova-state {ERROR | SHUTOFF}`	Optional	Displays OpenStack instances in the `ERROR` or `SHUTOFF` state only.
`--vc-state {poweredOn | poweredOff | suspended}`	Optional	Displays OpenStack instances in the specified state that are powered on, powered off, or suspended in vCenter Server.

You can also run `viocli get -h` or `viocli get --help` to display the parameters for the command.

Comando viocli import

Utilice el comando `viocli import` para importar certificados en la implementación.

El comando `viocli import` usa la siguiente sintaxis.

```
viocli import certificate -d cert-dir [-v]
```

Parámetro	Obligatorio u opcional	Descripción
`-d` *cert-dir* o `--folder` *cert-dir*	Obligatorio	Directorio que contiene los certificados que desea importar.
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli import -h` o `viocli import --help` para mostrar los parámetros del comando.

Comando viocli migrate

Utilice el comando `viocli migrate` para migrar recursos de la implementación.

El comando `viocli migrate` es compatible con diversas acciones para realizar diferentes tareas. Los siguientes parámetros se aplican a todas las acciones.

Parámetro	Obligatorio u opcional	Descripción
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

Puede ejecutar `viocli migrate -h` o `viocli migrate --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 migrate fwaas -h` muestra los parámetros para la acción `fwaas`.

A continuación, se enumeran las acciones que admite `viocli migrate`.

`viocli migrate fwaas [–v]`

Actualiza los firewalls en la implementación desde Firewall como servicio (FWaaS) v1 a FWaaS v2.

`viocli volume–migrate {––volume–ids` *`volume1–uuid`*`... | ––source–dc` *`src–dc–name`* `––source–ds` *`src–ds–name`*`] dest–dc–name dest–ds–name [––ignore–storage–policy] [–v]`

Migra volúmenes de Cinder no asociados a otro almacén de datos.

Parámetro	Obligatorio u opcional	Descripción
`––volume–ids`	Obligatorio si no se utiliza `––source–dc` ni `––source–ds`.	UUID del volumen que desea migrar. Puede incluir varios UUID, separados por comas (,). Si desea migrar todos los volúmenes de un almacén de datos, use los parámetros `––source–dc` y `––source–ds` en lugar de este parámetro.
`––source–dc` *src-dc-name*	Obligatorio si no se utiliza `––volume–ids`.	Nombre del centro de datos que contiene los volúmenes que desea migrar. Este parámetro debe utilizarse junto con el parámetro `––source–ds`. Si solo desea migrar volúmenes especificados, no incluya este parámetro.
`––source–ds` *src-ds-name*	Obligatorio si no se utiliza `––volume–ids`.	Nombre del almacén de datos que contiene los volúmenes que desea migrar. Este parámetro debe utilizarse junto con el parámetro `––source–dc`. Si solo desea migrar volúmenes especificados, no incluya este parámetro.
dest-dc-name	Obligatorio	Nombre del centro de datos que contiene el almacén de datos al que desea migrar volúmenes.
dest-ds-name	Obligatorio	Nombre del almacén de datos al que desea migrar volúmenes.
`––ignore–storage–policy`	Opcional	Migra volúmenes al almacén de datos de destino, incluso si el almacén de datos no cumple con la directiva de almacenamiento del volumen.

Comando viocli prepare

Use el comando `viocli prepare` para preparar almacenes de datos para migración.

Nota Este comando no admite volúmenes de asociación múltiple.

El comando `viocli prepare` usa la siguiente sintaxis.

```
viocli prepare datastore dc–name ds–name [–v]
```

Parámetro	Obligatorio u opcional	Descripción
dc-name	Obligatorio	Nombre del centro de datos que contiene los volúmenes deseados.
ds-name	Obligatorio	Nombre del almacén de datos que contiene los volúmenes deseados.
–v o ––verbose	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli prepare –h` o `viocli prepare ––help` para mostrar los parámetros del comando.

Comando viocli reset

Utilice el comando `viocli reset` para restablecer instancias en la implementación.

El comando `viocli reset` usa la siguiente sintaxis.

```
viocli reset instances ––nova–state {ERROR | SHUTOFF} [––force] [–v]
```

Parámetro	Obligatorio u opcional	Descripción
`––nova–state {ERROR | SHUTOFF}`	Obligatorio	Restablece instancias de OpenStack en el estado `ERROR` o `SHUTOFF`.
`––force`	Opcional	Ejecuta el comando sin confirmación.
–v o `––verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli reset –h` o `viocli reset ––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 create backup`.

Para obtener más información, consulte Restaurar la implementación desde una copia de seguridad.

El comando `viocli restore` usa la siguiente sintaxis.

```
viocli restore deployment {–f config–file | –i | –o} [––skip–control–plane] [–t timeout] [–v]
```

Parámetro	Obligatorio u opcional	Descripción
–f *config-file* o `––file` *config-file*	Opcional	Ejecuta el comando mediante un archivo de configuración específico.
`–i` o `––interactive`	Opcional	Abre la plantilla de configuración en un editor de texto para poder introducir la información necesaria de forma interactiva. Después de introducir la información, guarde y salga del editor de texto para ejecutar el comando.

Parámetro	Obligatorio u opcional	Descripción
`-o` o `--out`	Opcional	Ejecuta el comando sin solicitar una confirmación.
`--skip-control-plane`	Opcional	Restaura solamente la implementación de OpenStack y no modifica la configuración actual del plano de control.
`-t` *timeout* o `--timeout` *timeout*	Opcional	Especifica el tiempo en segundos durante el cual `viocli` mostrará el progreso de la operación de restauración. Si no incluye este parámetro, se utilizará el valor predeterminado de 1800 segundos.
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli restore -h` o `viocli restore --help` para mostrar los parámetros del comando.

Comando viocli start

Utilice el comando `viocli start` para iniciar servicios en la implementación.

El comando `viocli start` usa la siguiente sintaxis.

```
viocli start services [-t timeout] [-v]
```

Parámetro	Obligatorio u opcional	Descripción
`-t` *timeout* o `--timeout` *timeout*	Opcional	Especifica el tiempo en segundos durante el cual `viocli` mostrará el progreso de la operación de inicio. Si no incluye este parámetro, se utilizará el valor predeterminado de 900 segundos.
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli start -h` o `viocli start --help` para mostrar los parámetros del comando.

Comando viocli stop

Use el comando `viocli stop` para detener servicios en la implementación.

El comando `viocli stop` usa la siguiente sintaxis.

```
viocli stop services [-t timeout] [-v]
```

Parámetro	Obligatorio u opcional	Descripción
`-t` *timeout* o `--timeout` *timeout*	Opcional	Especifica el tiempo en segundos durante el cual `viocli` mostrará el progreso de la operación de inicio. Si no incluye este parámetro, se utilizará el valor predeterminado de 900 segundos.
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli stop -h` o `viocli stop --help` para mostrar los parámetros del comando.

Comando viocli update

Utilice el comando `viocli update` para actualizar la configuración de recursos en la implementación. La configuración se carga en el editor de texto predeterminado para que la modifique.

El comando `viocli update` usa la siguiente sintaxis.

```
viocli update resource-type [resource-name] [--live-debug={true | false}] [--force] [-v]
```

Parámetro	Obligatorio u opcional	Descripción
resource-type	Obligatorio	Tipo de recurso que desea actualizar. Se aceptan los siguientes valores: ■ `aodh` ■ `barbican` ■ `ceilometer` ■ `ceilometeragent` ■ `cinder` ■ `deployment` ■ `designate` ■ `glance` ■ `gnocchi` ■ `heat` ■ `horizon` ■ `keystone` ■ `mariadb` ■ `memcached` ■ `neutron` ■ `nova` ■ `novacompute` ■ `panko` ■ `rabbitmq` ■ `swift` ■ `tenant-vdc`
resource-name	Opcional	Nombre del recurso que desea actualizar. Si solo está en ejecución una instancia del recurso deseado, este parámetro no es necesario.
`--live-debug={true | false}`	Opcional	Utilizado principalmente por Investigación y desarrollo durante el desarrollo para habilitar el modo de depuración en vivo en el recurso especificado. Para permitir la depuración, inicie el pod del recurso con "inactividad infinito" en lugar de iniciar el proceso principal. **Nota** La depuración en vivo provoca una interrupción del plano de control de los servicios que se están depurando. Para volver a las operaciones normales, utilice viocli para deshabilitar la depuración en vivo y espere a que se reinicien los pods. Se recomienda a los clientes que solo utilicen esta función bajo la dirección de los servicios técnicos de VMware.
`--force`	Opcional	Ejecuta el comando sin confirmación.
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

El siguiente parámetro adicional se aplica al recurso `deployment`.

Parámetro	Obligatorio u opcional	Descripción
`--enable-ha`	Obligatorio	Habilita el modo de alta disponibilidad (High Availability, HA) en la implementación.

Los siguientes parámetros adicionales se aplican al recurso `tenant-vdc`.

Parámetro	Obligatorio u opcional	Descripción
`--compute` *compute-node*	Obligatorio	Nodo informático que contiene el VDC de tenant.
`--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. 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.

También puede ejecutar `viocli update -h` o `viocli update --help` para mostrar los parámetros del comando.

Comando viocli version

Utilice el comando `viocli version` para mostrar la versión actual de VMware Integrated OpenStack.

El comando `viocli version` usa la siguiente sintaxis.

```
viocli version [-v]
```

Parámetro	Obligatorio u opcional	Descripción
`-v` o `--verbose`	Opcional	Muestra los resultados en modo detallado.

También puede ejecutar `viocli version -h` o `viocli version --help` para mostrar los parámetros del comando.