Manos a la obra

Cloud Manager 3.7

NetApp
March 25, 2024

Tabla de contenidos

Manos a la obra

Información general sobre la implementación

Antes de empezar, es posible que desee comprender mejor las opciones que existen para poner en marcha Cloud Manager y Cloud Volumes ONTAP.

Instalación de Cloud Manager

Se necesita software Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP. Puede implementar Cloud Manager en cualquiera de las siguientes ubicaciones:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform

  Cloud Manager debe estar en Google Cloud Platform cuando se ponga en marcha Cloud Volumes ONTAP en GCP.

- Cloud de IBM
- En su propia red

La forma en que ponga en marcha Cloud Manager depende de la ubicación que elija:

Ubicación de Cloud Manager	Cómo poner en marcha Cloud Manager
AWS	1. "Ponga en marcha Cloud Manager desde NetApp Cloud Central" (recomendado) 2. "Ponga en marcha desde AWS Marketplace" 3. "Descargue e instale el software en un host Linux"
AWS C2S	"Ponga en marcha Cloud Manager desde AWS Intelligence Community Marketplace"
Azure región generalmente disponible	1. "Ponga en marcha Cloud Manager desde NetApp Cloud Central" (recomendado) 2. "Ponga en marcha desde Azure Marketplace" 3. "Descargue e instale el software en un host Linux"
Gobierno de Azure	"Ponga en marcha Cloud Manager desde Azure US Government Marketplace"
Azure Alemania	"Descargue e instale el software en un host Linux"

Ubicación de Cloud Manager	Cómo poner en marcha Cloud Manager
Google Cloud Platform	1. "Ponga en marcha Cloud Manager desde NetApp Cloud Central" (recomendado) 2. "Descargue e instale el software en un host Linux" No puede poner en marcha Cloud Manager en Google Cloud desde GCP Marketplace
Cloud de IBM	"Descargue e instale el software en un host Linux"
Red local	"Descargue e instale el software en un host Linux"

Configuración de Cloud Manager

Puede que desee realizar una configuración adicional después de instalar Cloud Manager, como añadir cuentas de proveedor de cloud adicionales, instalar un certificado HTTPS, etc.

- "Configurar la cuenta de Cloud Central"
- "Añadiendo cuentas de AWS a Cloud Manager"
- "Adición de cuentas de Azure a Cloud Manager"
- "Instalar un certificado HTTPS"
- "Configuración de AWS KMS"

Puesta en marcha de Cloud Volumes ONTAP

Después de poner en marcha Cloud Manager, puede empezar a poner en marcha Cloud Volumes ONTAP en su proveedor de cloud.

"Introducción a AWS", "Introducción a Azure", y. "Introducción a GCP" Proporcionar instrucciones para poner en funcionamiento Cloud Volumes ONTAP rápidamente. Si necesita ayuda adicional, consulte lo siguiente:

- "Configuraciones compatibles para Cloud Volumes ONTAP 9.7 en AWS"
- "Configuraciones compatibles para Cloud Volumes ONTAP 9.7 en Azure"
- "Configuraciones admitidas para Cloud Volumes ONTAP 9.7 en GCP"
- "Planificación de la configuración"
- "Inicio de Cloud Volumes ONTAP en AWS"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Lanzamiento de Cloud Volumes ONTAP en GCP"

Introducción a Cloud Volumes ONTAP en AWS

Empiece a usar Cloud Volumes ONTAP configurando AWS e inicie el software Cloud Manager desde NetApp Cloud Central. Está disponible una prueba gratuita de 30 días para el primer sistema Cloud Volumes ONTAP que se lanza en AWS.

Configure su red

1. Habilite el acceso a Internet de salida desde el VPC de destino, de modo que Cloud Manager y Cloud Volumes ONTAP puedan ponerse en contacto con varios extremos.

   Este paso es importante porque Cloud Manager no puede poner en marcha Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "Cloud Manager" y.. "Cloud Volumes ONTAP".

2. Configure un extremo de VPC con el servicio S3.

   Se requiere un extremo de VPC si desea organizar en niveles los datos inactivos de Cloud Volumes ONTAP en el almacenamiento de objetos de bajo coste.

Proporcione los permisos de AWS necesarios

Al implementar Cloud Manager desde NetApp Cloud Central, tiene que utilizar una cuenta de AWS con permisos para implementar la instancia.

1. Vaya a la consola AWS IAM y cree una política copiando y pegando el contenido de "Política central de Cloud de NetApp para AWS".
2. Adjunte la política al usuario del IAM.

Suscríbase desde el AWS Marketplace

"Suscríbase a Cloud Manager desde AWS Marketplace" Para garantizar que no se interrumpe el servicio una vez que finaliza la prueba gratuita de Cloud Volumes ONTAP. A partir de esta suscripción se le cobrará cada sistema de Cloud Volumes ONTAP PAYGO que cree y cada función complementaria que habilite.

Si inicia Cloud Volumes ONTAP con su propia licencia (BYOL), "Después, tendrá que suscribirse a esta oferta en AWS Marketplace".

Inicie Cloud Manager desde NetApp Cloud Central

Se necesita software Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP. Se tarda unos pocos minutos en iniciar una instancia de Cloud Manager desde "Cloud Central".

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Una vez que Cloud Manager esté listo, solo tiene que hacer clic en Create, seleccionar el tipo de sistema que le gustaría iniciar y completar los pasos del asistente. Tras 25 minutos, el primer sistema Cloud Volumes ONTAP debe estar listo para funcionar.

Vea el siguiente vídeo para conocer estos pasos:

► https://docs.netapp.com/es-es/occm37//media/video_getting_started_aws.mp4 *(video)*

Enlaces relacionados

- "Evaluación"
- "Requisitos de red para Cloud Manager"
- "Requisitos de red para Cloud Volumes ONTAP en AWS"
- "Reglas de grupos de seguridad para AWS"
- "Añadiendo cuentas de AWS a Cloud Manager"
- "Qué hace Cloud Manager con los permisos de AWS"
- "Inicio de Cloud Volumes ONTAP en AWS"
- "Ejecute Cloud Manager desde AWS Marketplace"

Introducción a Cloud Volumes ONTAP en Azure

Empiece a usar Cloud Volumes ONTAP configurando Azure y, a continuación, ponga en marcha el software Cloud Manager desde Cloud Central de NetApp. Hay disponibles instrucciones adicionales para implementar Cloud Manager en "Regiones gubernamentales de Azure EE. UU" y en "Regiones de Azure Alemania".

Configure su red

Habilite el acceso saliente a Internet desde la red virtual de destino para que Cloud Manager y Cloud Volumes ONTAP puedan ponerse en contacto con varios extremos.

Este paso es importante porque Cloud Manager no puede implementar Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "Cloud Manager" y.. "Cloud Volumes ONTAP".

Proporcione los permisos de Azure necesarios

Al poner en marcha Cloud Manager desde NetApp Cloud Central, necesita utilizar una cuenta de Azure con permisos para implementar la máquina virtual de Cloud Manager.

1. Descargue el "Política Cloud Central de NetApp para Azure".
2. Modifique el archivo JSON añadiendo el ID de suscripción de Azure al campo "AssignableScopes".
3. Utilice el archivo JSON para crear una función personalizada en Azure denominada *Azure SetupAsService*.

   Ejemplo: **Az role definition create --role-definition C:\Policy_for_Setup_as_Service_Azure.json**

4. En el portal de Azure, asigne la función personalizada al usuario que pondrá en marcha Cloud Manager desde Cloud Central.

Inicie Cloud Manager desde NetApp Cloud Central

Se necesita software Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP. Se tarda unos

pocos minutos en iniciar una instancia de Cloud Manager desde "Cloud Central".

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Una vez que Cloud Manager esté listo, haga clic en Create, seleccione el tipo de sistema que desea implementar y complete los pasos del asistente. Tras 25 minutos, el primer sistema Cloud Volumes ONTAP debe estar listo para funcionar.

Enlaces relacionados

- "Evaluación"
- "Requisitos de red para Cloud Manager"
- "Requisitos de red para Cloud Volumes ONTAP en Azure"
- "Reglas de grupos de seguridad para Azure"
- "Adición de cuentas de Azure a Cloud Manager"
- "Qué hace Cloud Manager con permisos de Azure"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Ejecute Cloud Manager desde Azure Marketplace"

Introducción a Cloud Volumes ONTAP en Google Cloud Platform

Empiece a usar Cloud Volumes ONTAP configurando GCP y, a continuación, poniendo en marcha el software Cloud Manager de NetApp Cloud Central.

Cloud Manager debe instalarse en Google Cloud Platform para poder poner en marcha Cloud Volumes ONTAP en GCP.

Configure su red

Habilite el acceso a Internet de salida desde el VPC de destino, de modo que Cloud Manager y Cloud Volumes ONTAP puedan ponerse en contacto con varios extremos.

Este paso es importante porque Cloud Manager no puede poner en marcha Cloud Volumes ONTAP sin acceso saliente a Internet. Si necesita limitar la conectividad saliente, consulte la lista de puntos finales para "Cloud Manager" y.. "Cloud Volumes ONTAP".

Configure los permisos y proyectos de GCP

Asegúrese de que existen dos conjuntos de permisos:

1. Compruebe que el usuario de GCP que implementa Cloud Manager desde NetApp Cloud Central tiene los permisos en el "Política de Cloud Central para GCP".

   "Puede crear una función personalizada con el archivo YAML" y, a continuación, adjuntarlo al usuario. Deberá utilizar la línea de comandos gcloud para crear la función.

2. Configure una cuenta de servicio con los permisos que Cloud Manager necesita para crear y gestionar sistemas Cloud Volumes ONTAP en los proyectos.

   Esta cuenta de servicio se asociará a la máquina virtual de Cloud Manager en el paso 6.

   - "Crear un rol en GCP" esto incluye los permisos definidos en la "Política de Cloud Manager para GCP". De nuevo, deberá utilizar la línea de comandos gcloud.

     Los permisos contenidos en este archivo YAML son diferentes a los del paso 2a.

   - "Cree una cuenta de servicio de GCP y aplique el rol personalizado que acaba de crear".
   - Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, "Conceda el acceso añadiendo la cuenta de servicio con la nube La función de gerente de ese proyecto". Deberá repetir este paso con cada proyecto.

Configure GCP para la organización en niveles de datos

Deben cumplirse dos requisitos para agrupar los datos fríos en niveles de Cloud Volumes ONTAP 9.7 en un almacenamiento de objetos de bajo coste (un bucket de almacenamiento en cloud de Google):

1. "Cree una cuenta de servicio" Que tiene el rol de administrador de almacenamiento predefinido y la cuenta de servicio de Cloud Manager como usuario.

   Deberá seleccionar esta cuenta de servicio más adelante al crear un entorno de trabajo de Cloud Volumes ONTAP. Esta cuenta de servicio es diferente de la cuenta de servicio que creó en el paso 2.

2. "Configure la subred de Cloud Volumes ONTAP para acceso privado a Google".

Si desea utilizar la organización en niveles de datos con Cloud Volumes ONTAP 9.6, "a continuación, siga estos pasos".

Habilite las API de Google Cloud

"Habilite las siguientes API de Google Cloud en su proyecto". Estas API son necesarias para poner en marcha Cloud Manager y Cloud Volumes ONTAP.

- API de Cloud Deployment Manager V2
- API de Cloud Resource Manager
- API del motor de computación
- API de registro de Stackdriver

Suscríbase en el mercado de GCP

"Suscríbase a Cloud Volumes ONTAP en el mercado de GCP" para asegurarse de que no haya interrupción del servicio después de que finalice su prueba gratuita. Se le cobrará de esta suscripción por cada sistema Cloud Volumes ONTAP PAYGO que cree.

Inicie Cloud Manager desde NetApp Cloud Central

Se necesita software Cloud Manager para poner en marcha y gestionar Cloud Volumes ONTAP. Se tarda solo unos minutos en lanzar una instancia de Cloud Manager en GCP desde "Cloud Central".

Cuando elige GCP como proveedor de cloud, Google le pide que inicie sesión en su cuenta y que conceda permisos. Al hacer clic en "permitir", se concede acceso a las API de computación necesarias para implementar Cloud Manager.

Inicie Cloud Volumes ONTAP mediante Cloud Manager

Una vez que Cloud Manager esté listo, haga clic en Create, seleccione el tipo de sistema que desea implementar y complete los pasos del asistente. Tras 25 minutos, el primer sistema Cloud Volumes ONTAP debe estar listo para funcionar.

Enlaces relacionados

- "Evaluación"
- "Requisitos de red para Cloud Manager"
- "Requisitos de red para Cloud Volumes ONTAP en GCP"
- "Reglas de firewall para GCP"
- "Qué hace Cloud Manager con los permisos de GCP"
- "Lanzamiento de Cloud Volumes ONTAP en GCP"
- "Descargue e instale el software Cloud Manager en un host Linux"

Configure Cloud Manager

Configuración de espacios de trabajo y usuarios en la cuenta de Cloud Central

Cada sistema de Cloud Manager está asociado con una cuenta *de Cloud Central de NetApp*. Configure la cuenta de Cloud Central asociada con su sistema de Cloud Manager para que los usuarios puedan acceder a Cloud Manager e implementar sistemas Cloud Volumes ONTAP en espacios de trabajo. Solo tiene que agregar un usuario o agregar varios usuarios y espacios de trabajo.

La cuenta se mantiene en Cloud Central, por lo que cualquier cambio que haga estará disponible para otros sistemas de Cloud Manager y para otros servicios de datos en el cloud de NetApp. "Obtenga más información sobre cómo funcionan las cuentas de Cloud Central".

Agregar espacios de trabajo

En Cloud Manager, los espacios de trabajo permiten aislar un conjunto de entornos de trabajo de otros entornos de trabajo y de otros usuarios. Por ejemplo, puede crear dos espacios de trabajo y asociar usuarios independientes a los espacios de trabajo.

Pasos

1. Haga clic en **Configuración de cuenta**.

2. Haga clic en **espacios de trabajo**.
3. Haga clic en **Agregar nuevo espacio de trabajo**.
4. Introduzca un nombre para el área de trabajo y haga clic en **Agregar**.

Después de terminar

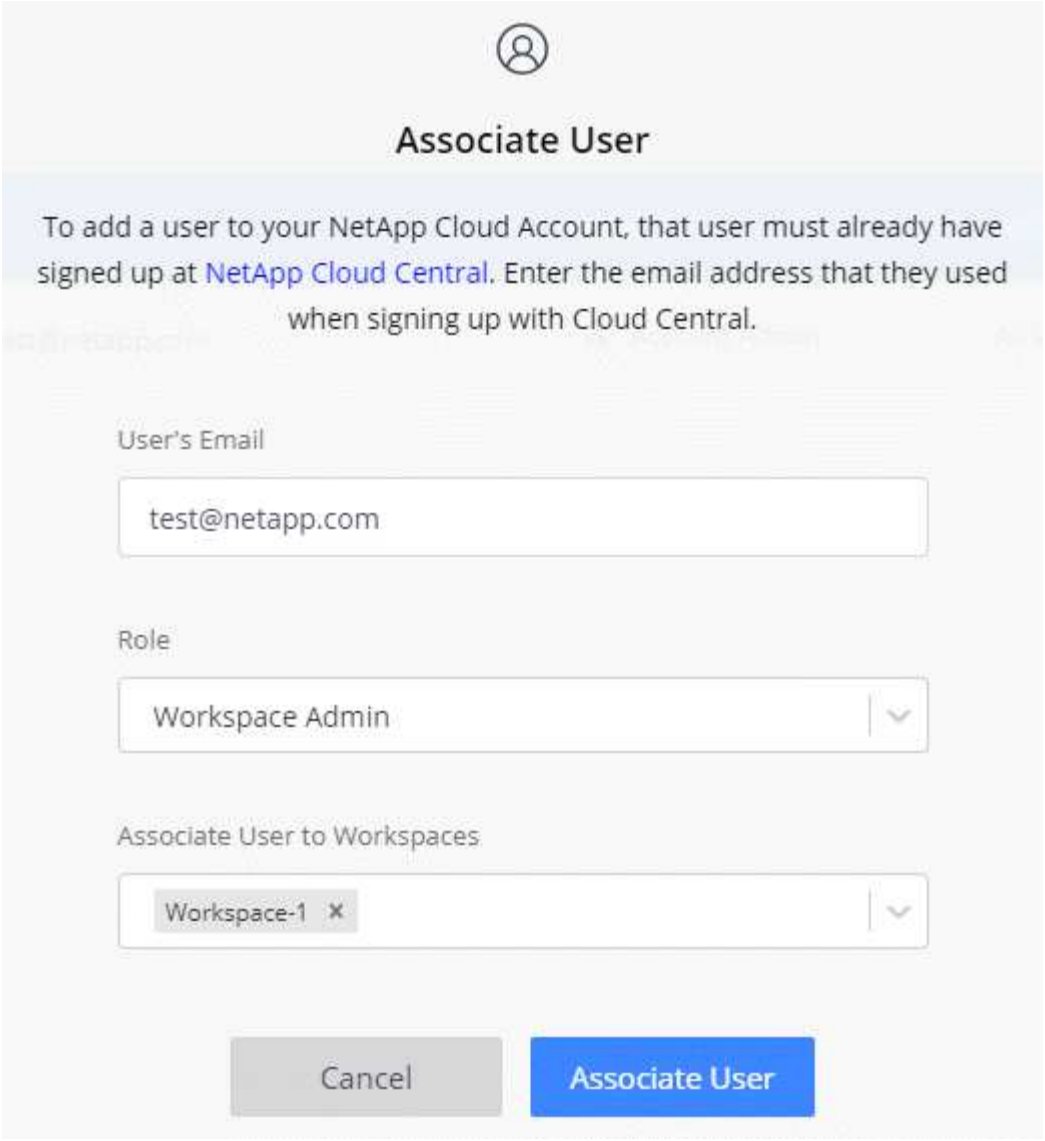
Ahora puede asociar usuarios y conectores de servicio al espacio de trabajo.

Adición de usuarios

Asocie los usuarios de Cloud Central a la cuenta de Cloud Central para que esos usuarios puedan crear y gestionar entornos de trabajo en Cloud Manager.

Pasos

1. Si el usuario aún no lo ha hecho, pida al usuario que vaya a. "Cloud Central de NetApp" y crear una cuenta.
2. En Cloud Manager, haga clic en **Configuración de cuenta**.
3. En la ficha usuarios, haga clic en **Usuario asociado**.
4. Introduzca la dirección de correo electrónico del usuario y seleccione un rol para el usuario:
   - **Administrador de cuentas**: Puede realizar cualquier acción en Cloud Manager.
   - **Administración de área de trabajo**: Puede crear y administrar recursos en áreas de trabajo asignadas.
5. Si ha seleccionado Administrador de área de trabajo, seleccione una o más áreas de trabajo para asociarlas a ese usuario.



6. Haga clic en **Usuario asociado**.

Resultado

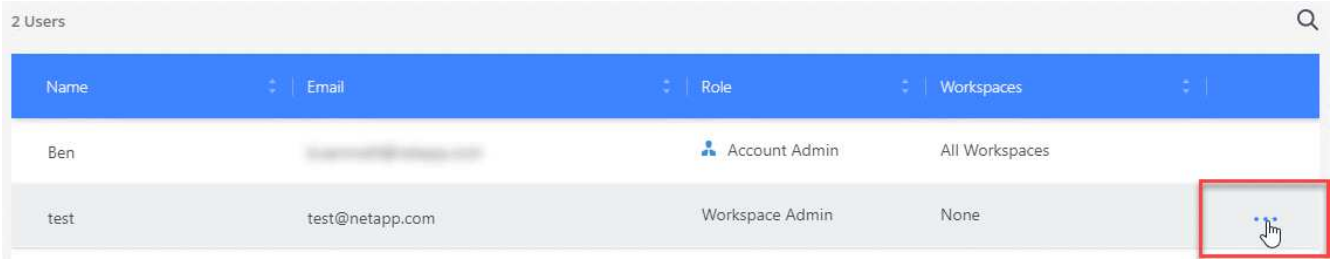
El usuario debe recibir un correo electrónico de Cloud Central de NetApp titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a Cloud Manager.

Asociación de administradores de área de trabajo con áreas de trabajo

Puede asociar los administradores de área de trabajo a espacios de trabajo adicionales en cualquier momento. La asociación del usuario les permite crear y ver los entornos de trabajo en ese espacio de trabajo.

Pasos

1. Haga clic en **Configuración de cuenta**.
2. Haga clic en el menú de acción de la fila correspondiente al usuario.



3. Haga clic en **Administrar espacios de trabajo**.
4. Seleccione uno o más espacios de trabajo y haga clic en **aplicar**.

Resultado

Ahora el usuario puede acceder a estos espacios de trabajo desde Cloud Manager, siempre y cuando el conector del servicio también esté asociado a los espacios de trabajo.

Asociación de conectores de servicio con áreas de trabajo

Un conector de servicio forma parte del sistema Cloud Manager. Se ejecuta en la instancia de máquina virtual que se implementó en su proveedor de cloud o en un host en las instalaciones que configuró. Debe asociar este conector de servicio a espacios de trabajo para que los administradores de espacio de trabajo puedan acceder a estos espacios de trabajo desde Cloud Manager.

Si sólo tiene Administradores de cuentas, no es necesario asociar el conector de servicio a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todos los espacios de trabajo de Cloud Manager de forma predeterminada.

"Obtenga más información sobre usuarios, espacios de trabajo y conectores de servicio".

Pasos

1. Haga clic en **Configuración de cuenta**.
2. Haga clic en **Service Connector**.
3. Haga clic en **Administrar áreas de trabajo** para el conector de servicio que desea asociar.
4. Seleccione uno o más espacios de trabajo y haga clic en **aplicar**.

Resultado

Los administradores de área de trabajo ahora pueden acceder a los espacios de trabajo asociados, siempre que el usuario también esté asociado al área de trabajo.

Configurar y añadir cuentas de AWS en Cloud Manager

Si desea poner en marcha Cloud Volumes ONTAP en diferentes cuentas de AWS, debe proporcionar los permisos necesarios y añadir los detalles a Cloud Manager. La forma en la que proporcione los permisos depende de si desea proporcionar a Cloud Manager claves de AWS o el ARN del rol en una cuenta de confianza.

Cuando pone en marcha Cloud Manager desde Cloud Central, Cloud Manager agrega automáticamente la cuenta de AWS en la que implementó Cloud Manager. No se agrega una cuenta inicial si instaló manualmente el software Cloud Manager en un sistema existente. "Obtenga más información acerca de los permisos y las cuentas de AWS".

opciones

- Concesión de permisos proporcionando claves AWS
- Otorgar permisos asumiendo roles de IAM en otras cuentas

Concesión de permisos proporcionando claves AWS

Si desea proporcionar a Cloud Manager claves AWS para un usuario IAM, debe conceder los permisos necesarios a ese usuario. La política de IAM de Cloud Manager define las acciones y los recursos de AWS que se permite el uso de Cloud Manager.

Pasos

1. Descargue la política de IAM de Cloud Manager desde el "Directivas de Cloud Manager".
2. Desde la consola de IAM, cree su propia política copiando y pegando el texto de la política IAM de Cloud Manager.

   "Documentación de AWS: Crear políticas de IAM"

3. Asocie la política a un rol de IAM o a un usuario de IAM.
   - "Documentación de AWS: Crear roles de IAM"
   - "Documentación de AWS: Adición y eliminación de políticas de IAM"

Resultado

La cuenta ahora tiene los permisos necesarios. Ahora puede añadirlo a Cloud Manager.

Otorgar permisos asumiendo roles de IAM en otras cuentas

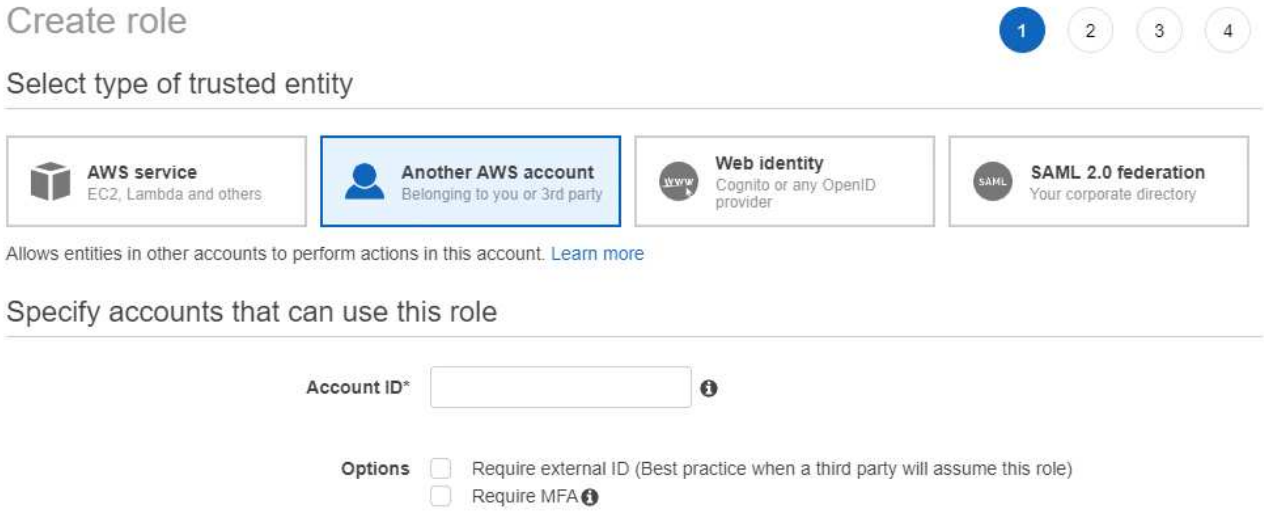
Puede configurar una relación de confianza entre la cuenta de AWS de origen en la que implementó la instancia de Cloud Manager y otras cuentas de AWS mediante los roles de IAM. A continuación, debe proporcionar a Cloud Manager el ARN de las funciones de IAM de las cuentas de confianza.

Pasos

1. Vaya a la cuenta de destino donde desea implementar Cloud Volumes ONTAP y cree una función IAM seleccionando **otra cuenta de AWS**.

   No olvide hacer lo siguiente:

   - Introduzca el ID de la cuenta en la que reside la instancia de Cloud Manager.
   - Adjunte la política IAM de Cloud Manager, que está disponible en la "Directivas de Cloud Manager".



2. Vaya a la cuenta de origen donde reside la instancia de Cloud Manager y seleccione la función IAM que se adjunta a la instancia.

   a. Haga clic en **Relaciones de confianza > Editar relación de confianza**.

   b. Agregue la acción "sts:AssumeRole" y el ARN de la función que creó en la cuenta de destino.

   ejemplo

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Resultado

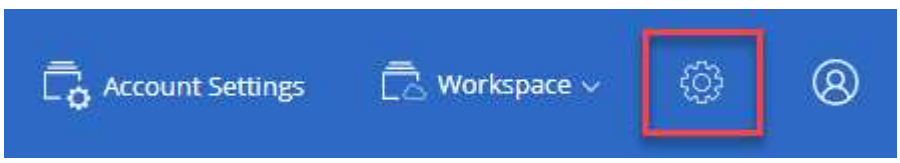
La cuenta ahora tiene los permisos necesarios. Ahora puede añadirlo a Cloud Manager.

Añadiendo cuentas de AWS a Cloud Manager

Después de proporcionar una cuenta de AWS con los permisos necesarios, puede añadir la cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Pasos

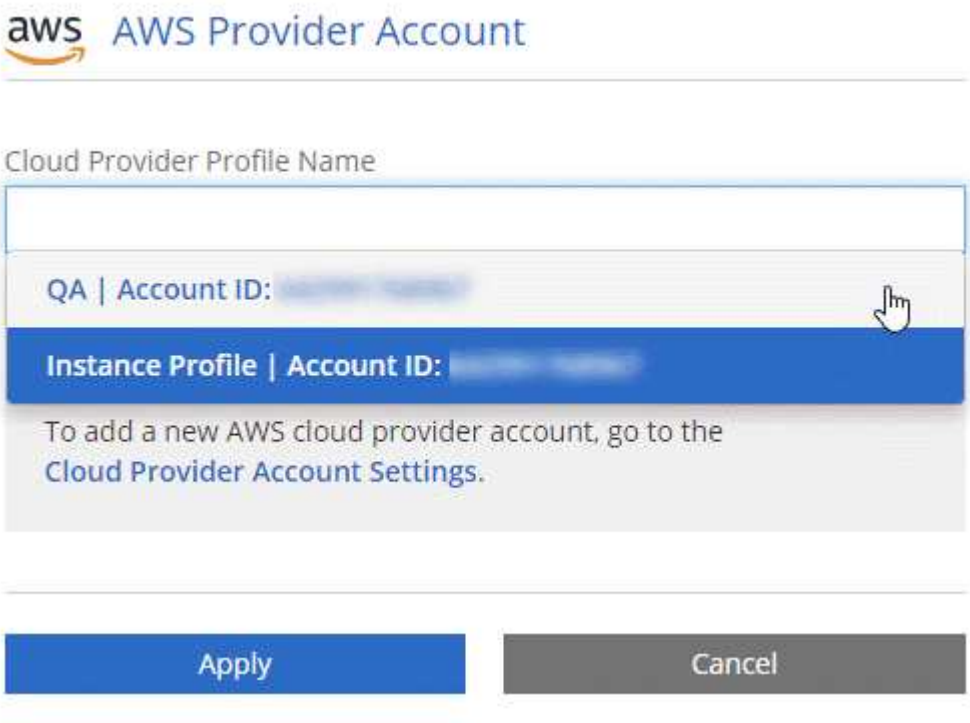
1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Proveedor de cloud y Cuentas de soporte**.



2. Haga clic en **Agregar nueva cuenta** y seleccione **AWS**.
3. Elija si desea proporcionar las claves AWS o el ARN de un rol de IAM de confianza.
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **Crear cuenta**.

Resultado

Ahora puede cambiar a otra cuenta desde la página Details y Credentials al crear un nuevo entorno de trabajo:



Configurar y añadir cuentas de Azure a Cloud Manager

Si desea poner en marcha Cloud Volumes ONTAP en diferentes cuentas de Azure, tendrá que proporcionar los permisos necesarios para esas cuentas y, a continuación, añadir detalles acerca de las cuentas a Cloud Manager.

Cuando se pone en marcha Cloud Manager desde Cloud Central, Cloud Manager agrega automáticamente la cuenta de Azure en la que implementó Cloud Manager. No se agrega una cuenta inicial si instaló manualmente el software Cloud Manager en un sistema existente. "Obtenga más información acerca de las cuentas y los permisos de Azure".

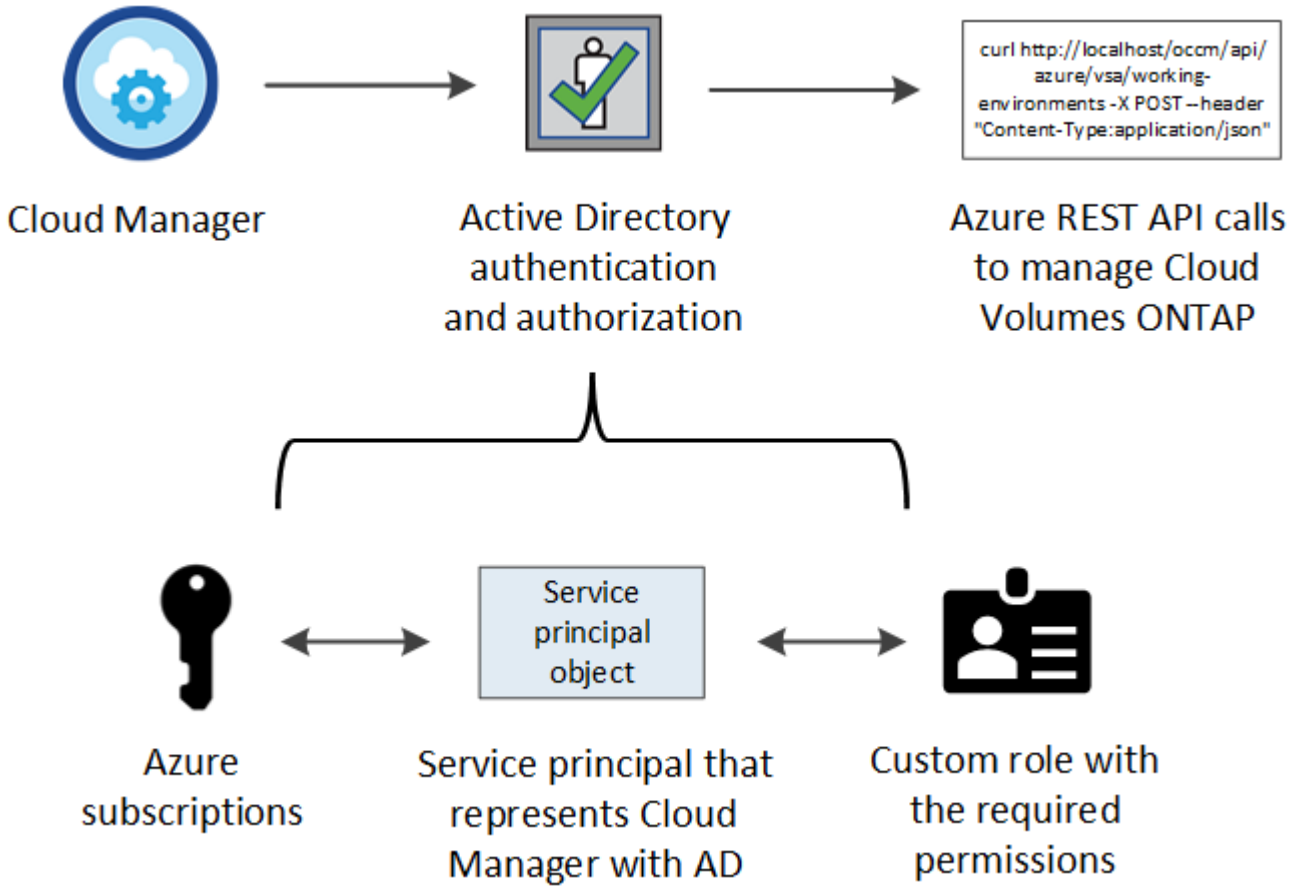
Concesión de permisos de Azure con un director de servicio

Cloud Manager necesita permisos para realizar acciones en Azure. Puede conceder los permisos requeridos a una cuenta de Azure creando y configurando un servicio principal en Azure Active Directory y obteniendo las credenciales de Azure que necesita Cloud Manager.

Acerca de esta tarea

La siguiente imagen muestra cómo Cloud Manager obtiene permisos para realizar operaciones en Azure. Un objeto principal de servicio, que está vinculado a una o varias suscripciones de Azure, representa Cloud

Manager en Azure Active Directory y se asigna a una función personalizada que permite los permisos necesarios.



Pasos

1. Cree una aplicación de Azure Active Directory.
2. Asigne la aplicación a una función.
3. Añada permisos de API de administración de servicios de Windows Azure.
4. Obtener el ID de aplicación y el ID de directorio.
5. Cree un secreto de cliente.

Crear una aplicación de Azure Active Directory

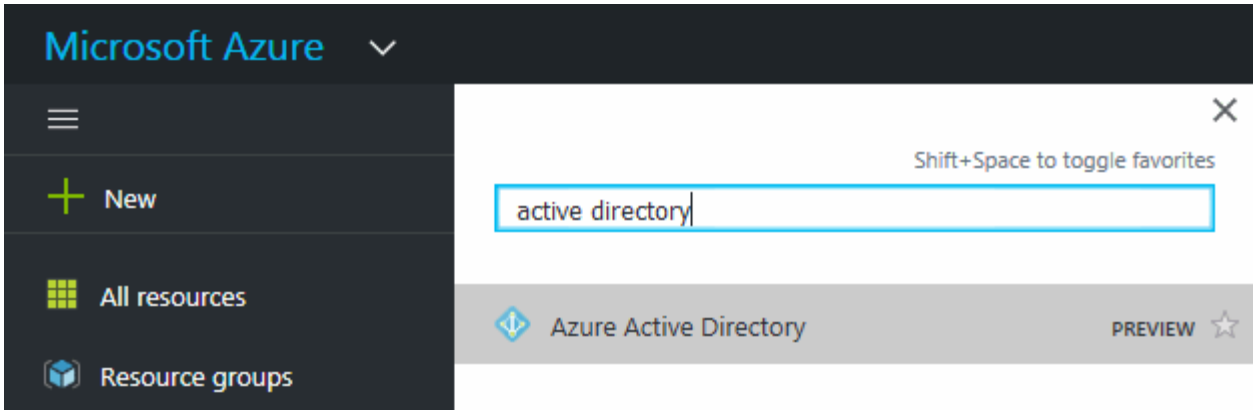
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que Cloud Manager pueda usar para el control de acceso basado en roles.

Antes de empezar

Debe tener los permisos adecuados en Azure para crear una aplicación de Active Directory y asignar la aplicación a un rol. Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios".

Pasos

1. Desde el portal de Azure, abra el servicio **Azure Active Directory**.



2. En el menú, haga clic en **App registrs**.
3. Haga clic en **Nuevo registro**.
4. Especificar detalles acerca de la aplicación:
   - **Nombre**: Introduzca un nombre para la aplicación.
   - **Tipo de cuenta**: Seleccione un tipo de cuenta (cualquiera funcionará con Cloud Manager).
   - **Redirigir URI**: Seleccione **Web** y, a continuación, escriba cualquier dirección URL; por ejemplo, https://url
5. Haga clic en **Registrar**.

Resultado

Ha creado la aplicación AD y el director de servicio.

Asignación de la aplicación a una función

Debe enlazar el principal del servicio a una o más suscripciones de Azure y asignarle el rol personalizado de operador de "OnCommand Cloud Manager" para que Cloud Manager tenga permisos en Azure.

Pasos

1. Crear un rol personalizado:

   a. Descargue el "Política de Azure de Cloud Manager".

   b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

   Debe añadir el ID para cada suscripción de Azure desde la cual los usuarios crearán sistemas Cloud Volumes ONTAP.

   ejemplo

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

   c. Use el archivo JSON para crear una función personalizada en Azure.

   El ejemplo siguiente muestra cómo crear una función personalizada con la CLI de Azure 2.0:

Az role definition create --role-definition C:\Policy_for_cloud_Manager_Azure_3.7.4.json

Ahora debe tener un rol personalizado denominado *OnCommand Cloud Manager Operator*.

2. Asigne la aplicación al rol:

   a. En el portal de Azure, abra el servicio **Suscripciones**.

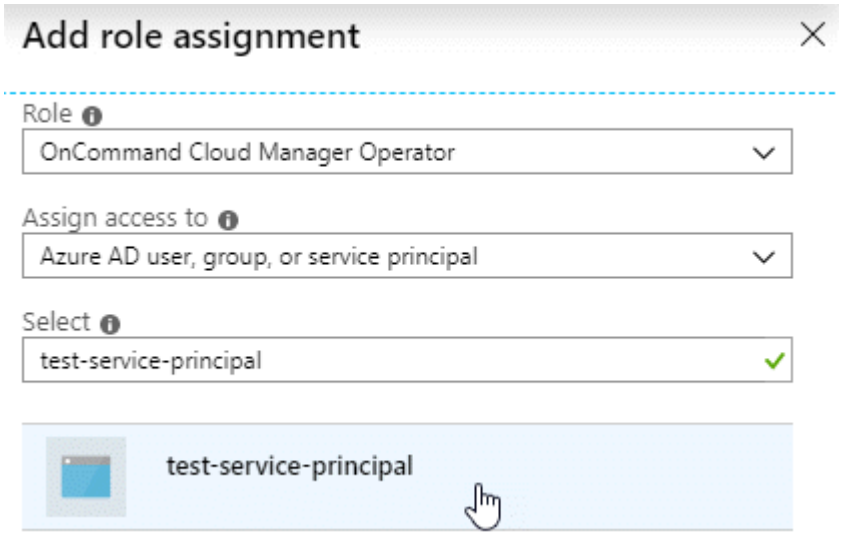
   b. Seleccione la suscripción.

   c. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.

   d. Seleccione el rol **operador de Cloud Manager de OnCommand**.

   e. Mantener seleccionado **usuario, grupo o principal de servicio de Azure AD**.

   f. Busque el nombre de la aplicación (no puede encontrarlo en la lista desplazándose).



   g. Seleccione la aplicación y haga clic en **Guardar**.

      El director de servicio de Cloud Manager ahora tiene los permisos de Azure necesarios para esa suscripción.

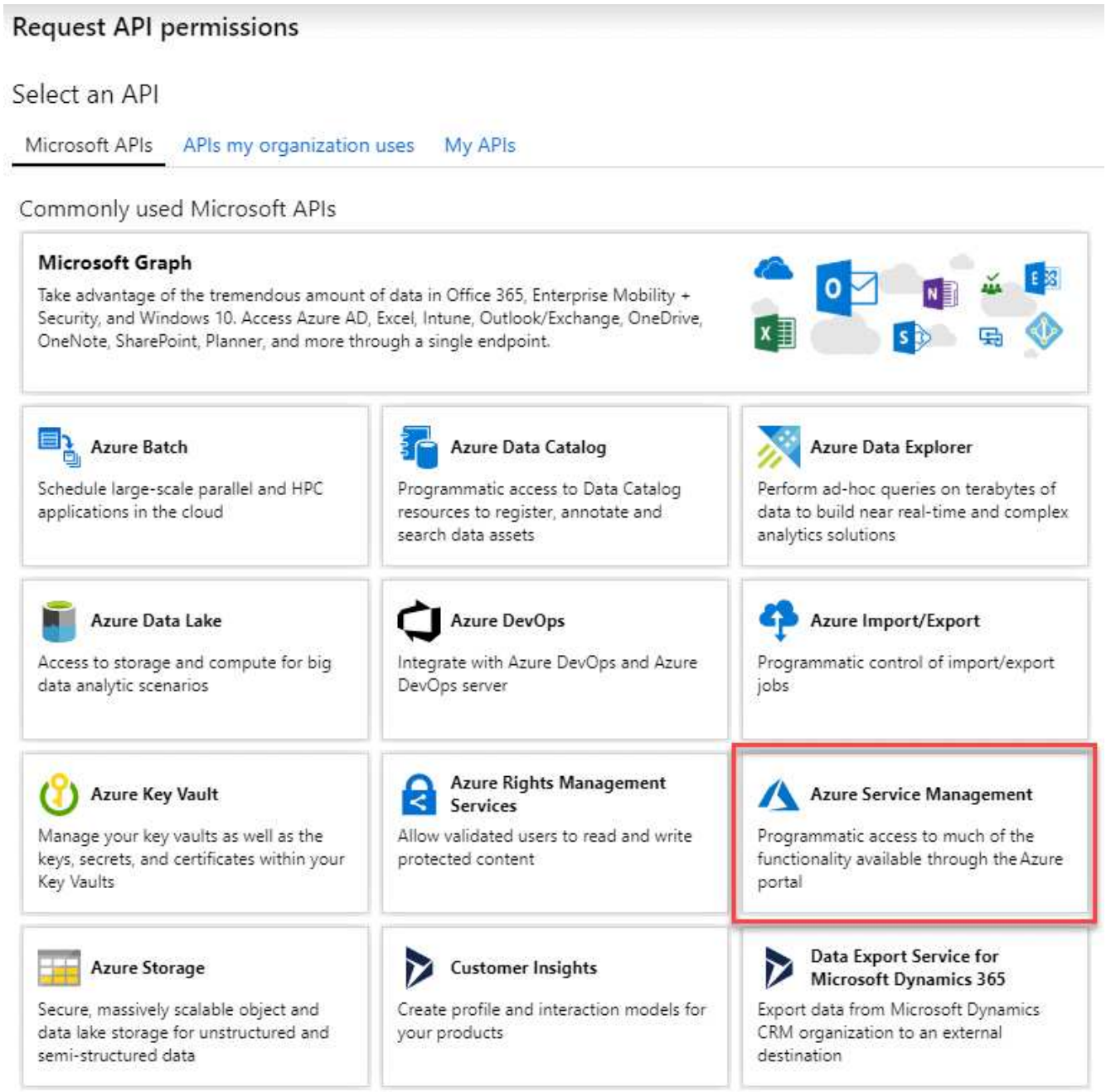
   Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. Cloud Manager le permite seleccionar la suscripción que desea utilizar al poner en marcha Cloud Volumes ONTAP.

Agregar permisos de API de administración de servicios de Windows Azure

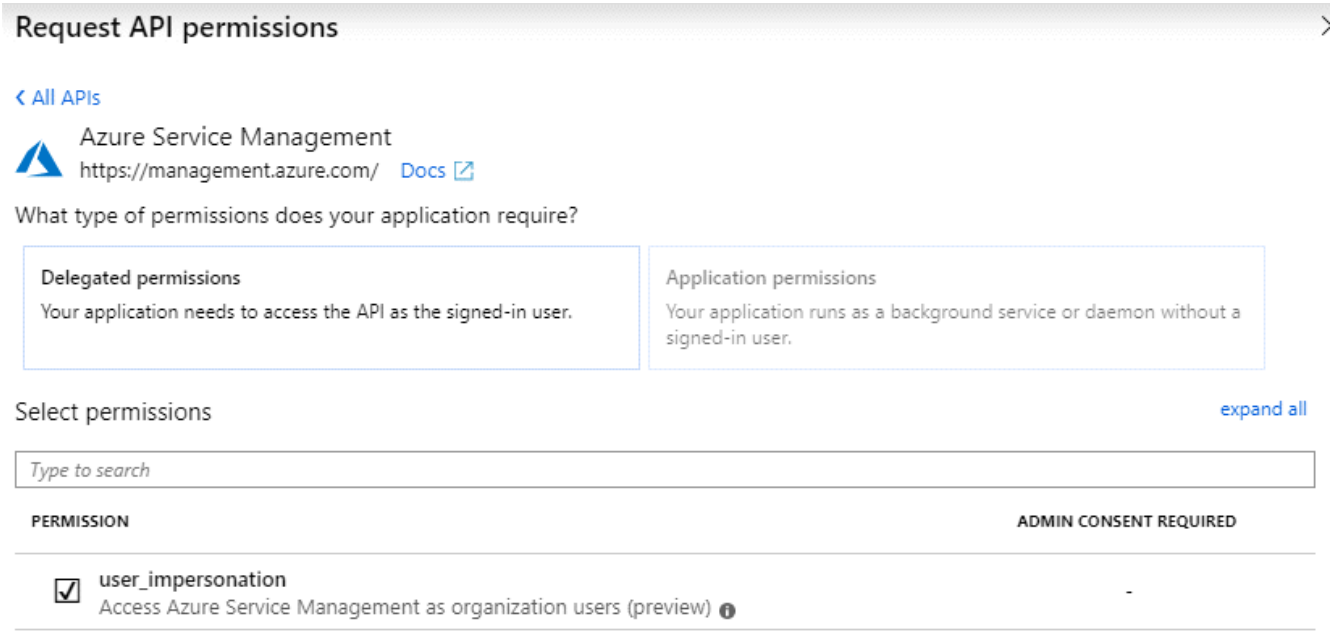
El principal de servicio debe tener permisos de "API de administración de servicios de Windows Azure".

Pasos

1. En el servicio **Azure Active Directory**, haga clic en **App registrs** y seleccione la aplicación.
2. Haga clic en **permisos de API > Agregar un permiso**.
3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.



4. Haga clic en **Access Azure Service Management como usuarios de la organización** y, a continuación, haga clic en **Agregar permisos**.

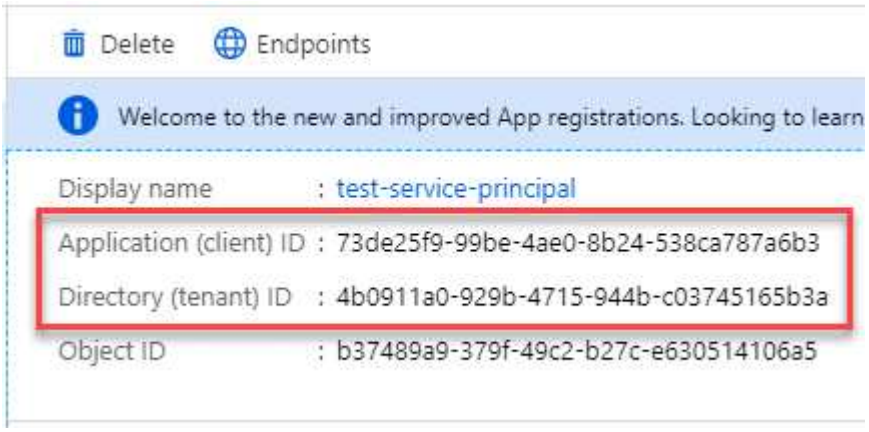


Obteniendo el ID de aplicación y el ID de directorio

Cuando agrega la cuenta de Azure a Cloud Manager, necesita proporcionar el ID de la aplicación (cliente) y el ID de directorio (inquilino) para la aplicación. Cloud Manager utiliza los ID para iniciar sesión mediante programación.

Pasos

1. En el servicio **Azure Active Directory**, haga clic en **App registrs** y seleccione la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



Crear un secreto de cliente

Debe crear un secreto de cliente y, a continuación, proporcionar a Cloud Manager el valor del secreto para que Cloud Manager pueda utilizarlo para autenticar con Azure AD.

Al agregar la cuenta a Cloud Manager, Cloud Manager hace referencia al secreto de cliente como la clave de aplicación.

Pasos

1. Abra el servicio **Azure Active Directory**.
2. Haga clic en **App registres** y seleccione su aplicación.
3. Haga clic en **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Haga clic en **Agregar**.
6. Copie el valor del secreto de cliente.

Resultado

Su principal de servicio ahora está configurado y debe haber copiado el ID de aplicación (cliente), el ID de directorio (arrendatario) y el valor del secreto de cliente. Necesita introducir esta información en Cloud Manager al añadir una cuenta de Azure.

Adición de cuentas de Azure a Cloud Manager

Después de proporcionar una cuenta de Azure con los permisos necesarios, puede añadir la cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

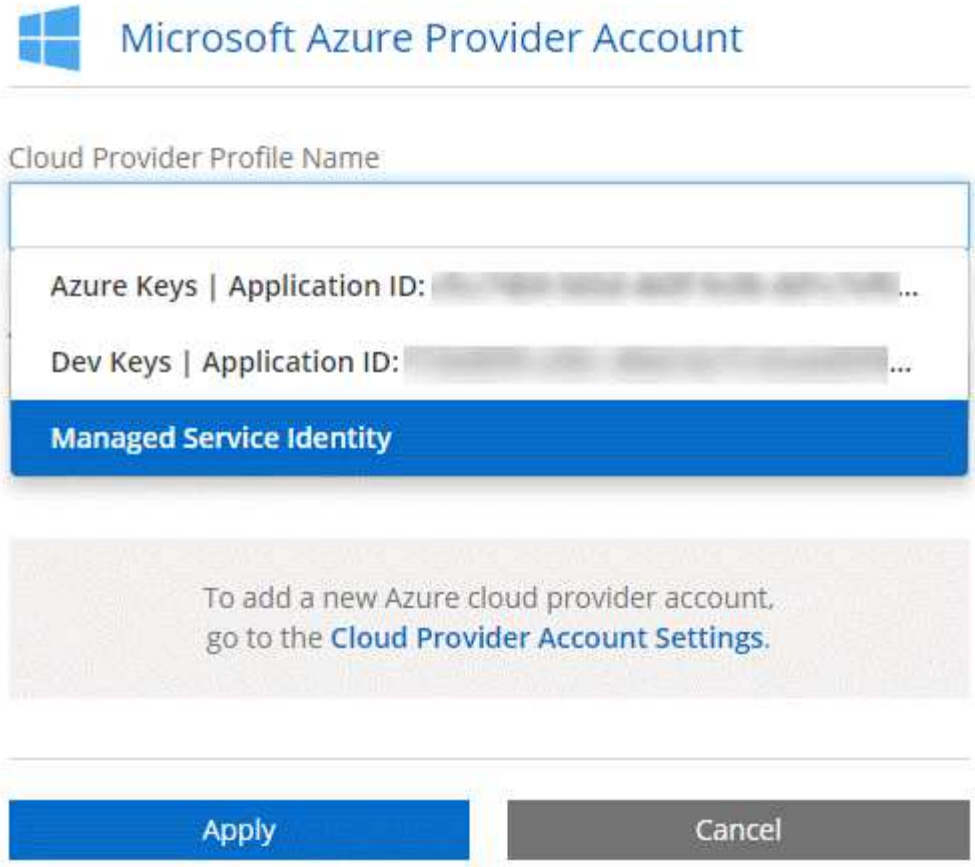
Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Proveedor de cloud y Cuentas de soporte**.

2. Haga clic en **Agregar nueva cuenta** y seleccione **Microsoft Azure**.
3. Introduzca la información acerca del director del servicio de Azure Active Directory que otorga los permisos necesarios:
   - ID de aplicación: Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - ID de inquilino (o ID de directorio): Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - Clave de aplicación (el secreto de cliente): Consulte Crear un secreto de cliente.
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **Crear cuenta**.

Resultado

Ahora puede cambiar a otra cuenta desde la página Details y Credentials al crear un nuevo entorno de trabajo:



Asociar suscripciones de Azure adicionales a una identidad administrada

Cloud Manager le permite elegir la cuenta y la suscripción de Azure en la que desee poner en marcha Cloud Volumes ONTAP. No puede seleccionar una suscripción de Azure diferente para la gestionada perfil de identidad a menos que asocie el "identidad administrada" con estas suscripciones.

Acerca de esta tarea

Una identidad administrada es "La cuenta inicial de Azure" Cuando pone en marcha Cloud Manager desde NetApp Cloud Central. Cuando implementó Cloud Manager, Cloud Central creó la función del operador de Cloud Manager de OnCommand y la asignó a la máquina virtual de Cloud Manager.

Pasos

1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar sistemas Cloud Volumes ONTAP.
3. Haga clic en **Control de acceso (IAM)**.
   a. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos:
      - Seleccione el rol **operador de Cloud Manager de OnCommand**.

        El nombre predeterminado que se proporciona en la es el operador de OnCommand Cloud Manager "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

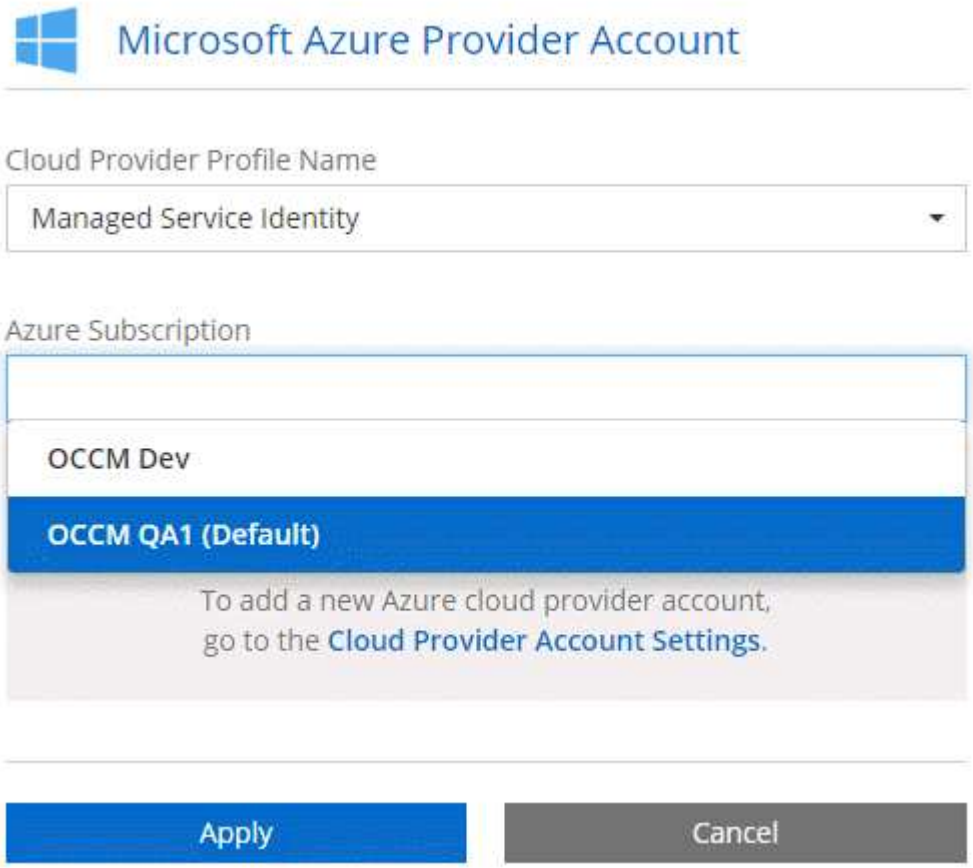
      - Asigne acceso a una **máquina virtual**.

- Seleccione la suscripción en la que se creó la máquina virtual de Cloud Manager.
- Seleccione la máquina virtual Cloud Manager.
- Haga clic en **Guardar**.

4. Repita estos pasos para suscripciones adicionales.

Resultado

Al crear un nuevo entorno de trabajo, ahora debe tener la posibilidad de seleccionar varias suscripciones de Azure para el perfil de identidad administrada.



Configuración y adición de cuentas de GCP a Cloud Manager

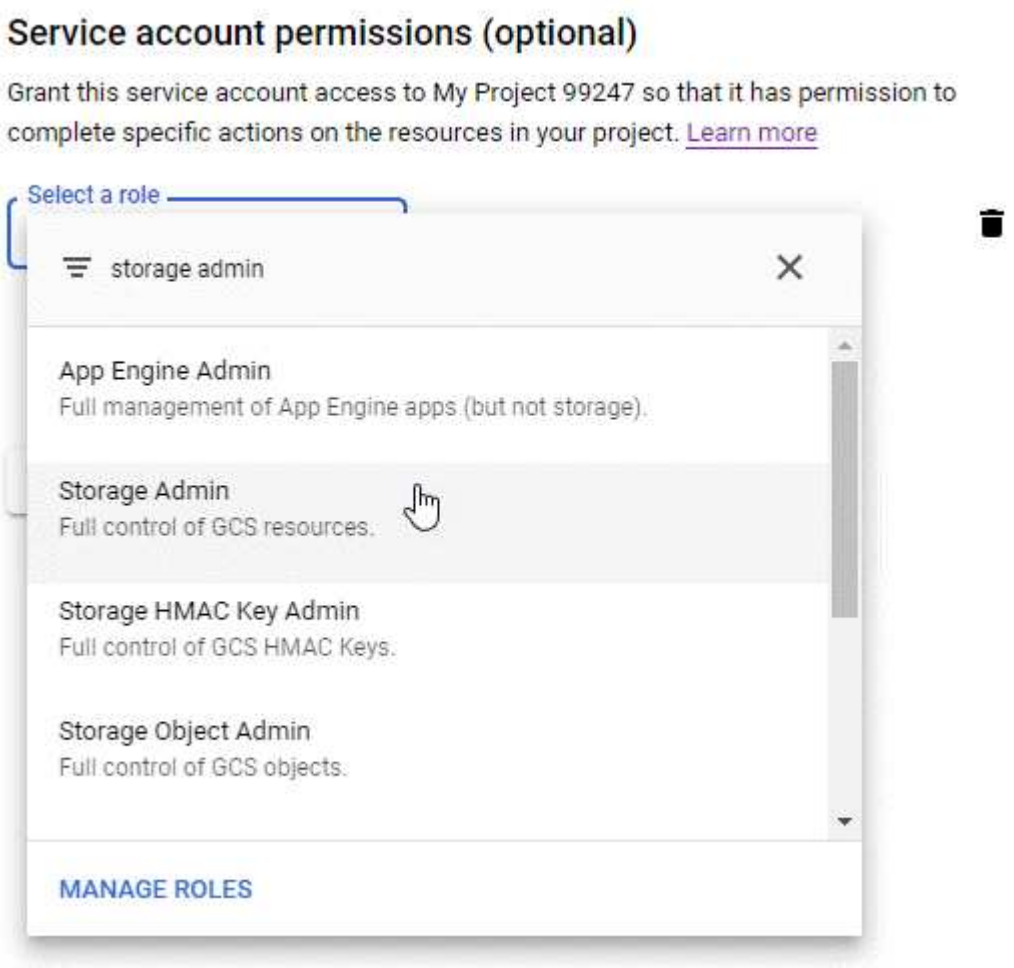
Si desea habilitar "organización en niveles de los datos" En un sistema Cloud Volumes ONTAP, debe proporcionar a Cloud Manager una clave de acceso al almacenamiento para una cuenta de servicio con permisos de administrador de almacenamiento. Cloud Manager utiliza las claves de acceso para configurar y gestionar un bucket de Cloud Storage para la organización de datos en niveles.

Configuración de una cuenta de servicio y claves de acceso para Google Almacenamiento en cloud

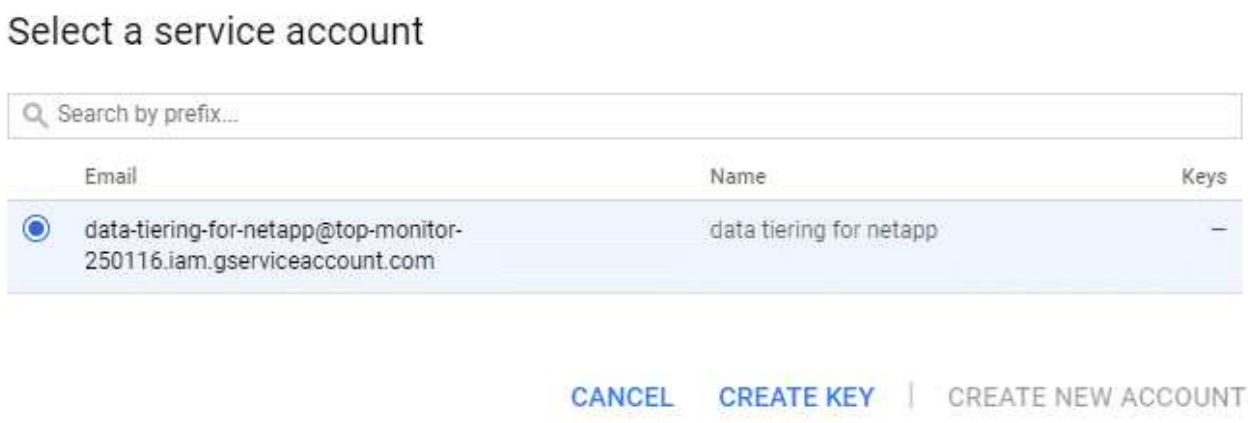
Una cuenta de servicio permite que Cloud Manager autentique y acceda a los bloques de almacenamiento en cloud que se utilizan para la organización en niveles de los datos. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

Pasos

1. Abra la consola GCP IAM y. "Cree una cuenta de servicio con el rol Storage Admin".



2. Vaya a. "Configuración de almacenamiento para GCP".
3. Si se le solicita, seleccione un proyecto.
4. Haga clic en la pestaña **interoperabilidad**.
5. Si aún no lo ha hecho, haga clic en **Activar acceso de interoperabilidad**.
6. En **claves de acceso para cuentas de servicio**, haga clic en **Crear una clave para una cuenta de servicio**.
7. Seleccione la cuenta de servicio que ha creado en el paso 1.



8. Haga clic en **Crear clave**.
9. Copie la clave de acceso y el secreto.

   Tendrá que introducir esta información en Cloud Manager cuando añada la cuenta de GCP para la organización en niveles de los datos.

Añadir una cuenta de GCP a Cloud Manager

Ahora que tiene una clave de acceso para una cuenta de servicio, puede agregarla a Cloud Manager.

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Proveedor de cloud y Cuentas de soporte**.

2. Haga clic en **Agregar nueva cuenta** y seleccione **GCP**.
3. Introduzca la clave de acceso y el secreto de la cuenta de servicio.

   Las claves permiten a Cloud Manager configurar un bucket de almacenamiento en cloud para la organización de datos en niveles.

4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **Crear cuenta**.

El futuro

Ahora puede habilitar la organización en niveles de los datos en volúmenes individuales al crearlos, modificarlos o replicarlos. Para obtener más información, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Pero antes de hacerlo, asegúrese de que la subred en la que reside Cloud Volumes ONTAP esté configurada para acceso privado a Google. Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración de Private Google Access".

Adición de cuentas del sitio de soporte de NetApp a Cloud Manager

Para añadir su cuenta del sitio de soporte de NetApp a Cloud Manager debe poner en marcha un sistema BYOL. También es necesario registrar sistemas de pago por uso y actualizar el software de ONTAP.

Vea el siguiente vídeo para descubrir cómo añadir cuentas del sitio de soporte de NetApp a Cloud Manager. O desplácese hacia abajo para leer los pasos.

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Pasos

1. Si aún no dispone de una cuenta en la página de soporte de NetApp, "regístrese para uno".
2. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Proveedor de cloud y Cuentas de soporte**.

3. Haga clic en **Agregar nueva cuenta** y seleccione **Sitio de soporte de NetApp**.
4. Escriba un nombre para la cuenta y, a continuación, escriba el nombre de usuario y la contraseña.
   - La cuenta debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal).
   - Si tiene pensado poner en marcha sistemas BYOL:
     - La cuenta debe estar autorizada para acceder a los números de serie de los sistemas BYOL.
     - Si ha adquirido una suscripción BYOL segura, será necesaria una cuenta de NSS segura.
5. Haga clic en **Crear cuenta.**

El futuro

Ahora los usuarios pueden seleccionar la cuenta al crear nuevos sistemas de Cloud Volumes ONTAP y al registrar los sistemas existentes.

- "Inicio de Cloud Volumes ONTAP en AWS"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Registro de sistemas de pago por uso"
- "Descubra cómo Cloud Manager gestiona los archivos de licencia"

Instalar un certificado HTTPS para obtener acceso seguro

De forma predeterminada, Cloud Manager utiliza un certificado autofirmado para el acceso HTTPS a la consola web. Puede instalar un certificado firmado por una CA, que proporciona una mejor protección de seguridad que un certificado autofirmado.

Pasos

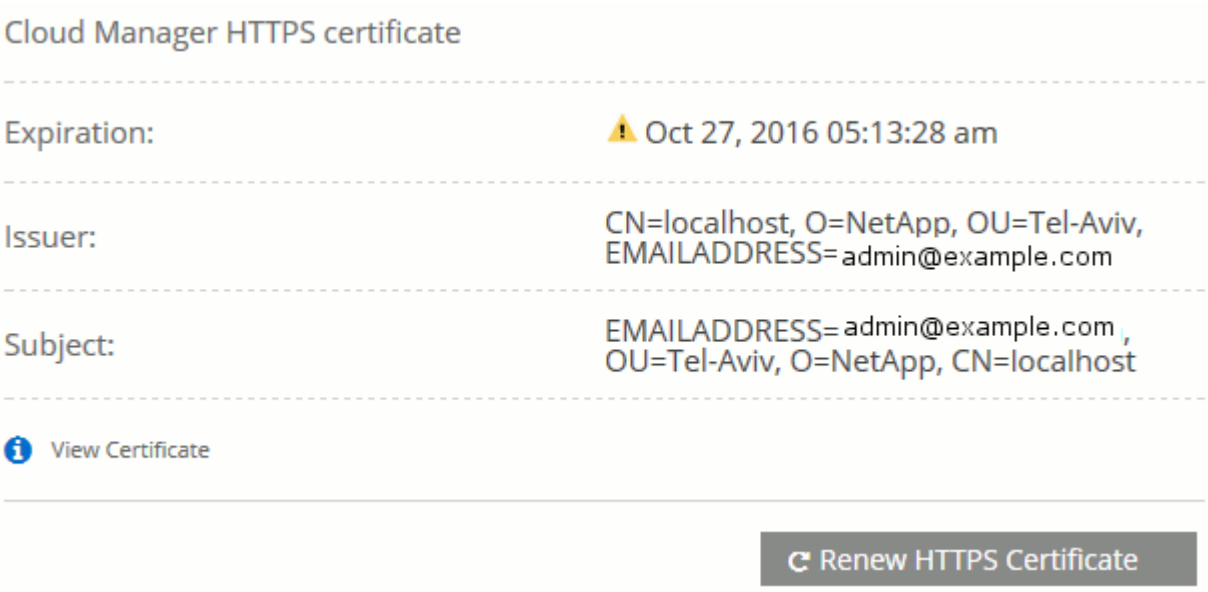
1. En la parte superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Configuración HTTPS**.

2. En la página HTTPS Setup, instale un certificado generando una solicitud de firma de certificación (CSR) o instalando su propio certificado firmado por una CA:

Opción	Descripción
Genere una CSR	a. Introduzca el nombre de host o DNS del host de Cloud Manager (su nombre común) y, a continuación, haga clic en **generar CSR**. Cloud Manager muestra una solicitud de firma de certificación. b. Utilice la CSR para enviar una solicitud de certificado SSL a una CA. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64. c. Copie el contenido del certificado firmado, péguelo en el campo Certificado y, a continuación, haga clic en **instalar**.
Instale su propio certificado firmado por CA	a. Seleccione **instalar certificado firmado por CA**. b. Cargue el archivo de certificado y la clave privada y, a continuación, haga clic en **instalar**. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.

Resultado

Cloud Manager ahora utiliza el certificado firmado por CA para proporcionar acceso HTTPS seguro. En la siguiente imagen se muestra un sistema Cloud Manager configurado para el acceso seguro:



Configuración de AWS KMS

Si desea usar el cifrado de Amazon con Cloud Volumes ONTAP, debe configurar el servicio de gestión de claves (KMS) de AWS.

Pasos

1. Asegúrese de que existe una clave maestra de cliente (CMK) activa.

   El CMK puede ser un CMK gestionado por AWS o un CMK gestionado por el cliente. Puede encontrarse en la misma cuenta de AWS que Cloud Manager y Cloud Volumes ONTAP, o en una cuenta de AWS diferente.

   "Documentación de AWS: Claves maestras de clientes (CMKs)"

2. Modifique la política de claves de cada CMK añadiendo el rol IAM que proporciona permisos a Cloud Manager como *key user*.

   La adición del rol IAM como usuario clave permite a Cloud Manager utilizar el CMK con Cloud Volumes ONTAP.

   "Documentación de AWS: Editar claves"

3. Si el CMK se encuentra en una cuenta de AWS diferente, realice los pasos siguientes:

   a. Vaya a la consola KMS desde la cuenta donde reside el CMK.

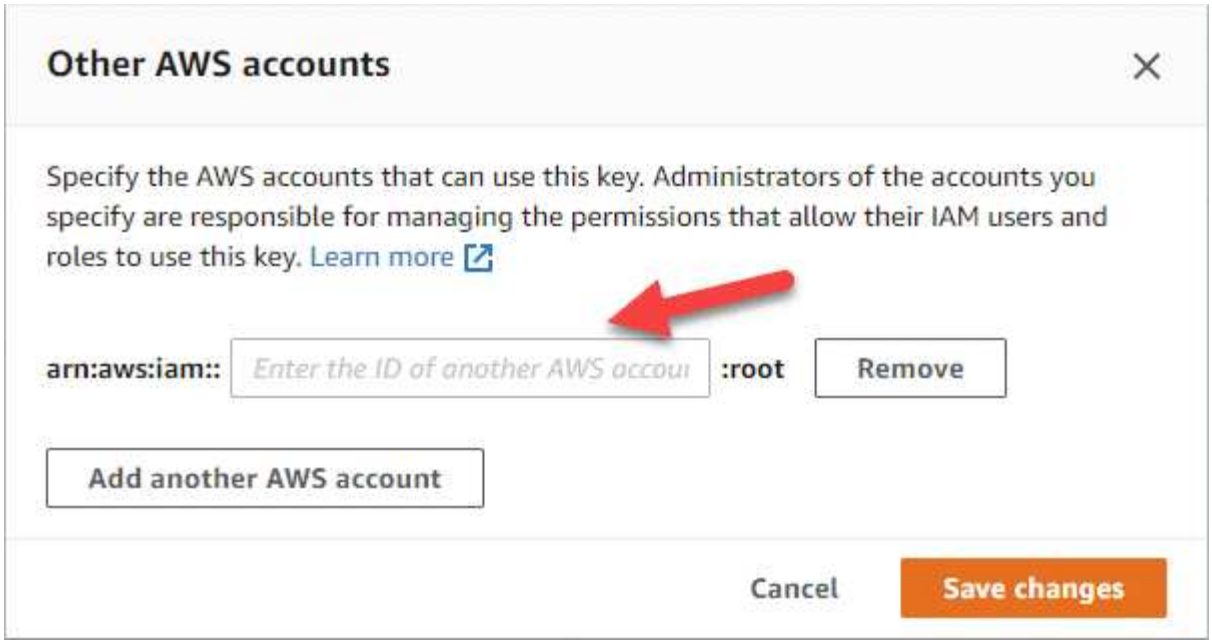
   b. Seleccione la tecla.

   c. En el panel **Configuración general**, copie el ARN de la clave.

      Deberá proporcionar el ARN al Cloud Manager cuando cree el sistema Cloud Volumes ONTAP.

   d. En el panel **otras cuentas de AWS**, agregue la cuenta de AWS que proporciona permisos a Cloud Manager.

      En la mayoría de los casos, esta es la cuenta en la que reside Cloud Manager. Si Cloud Manager no se instaló en AWS, sería la cuenta para la que proporcionó las claves de acceso de AWS a Cloud Manager.



e. Cambie ahora a la cuenta de AWS que proporciona permisos a Cloud Manager y abra la consola IAM.

f. Cree una política de IAM que incluya los permisos que se indican a continuación.

g. Asocie la política al rol de IAM o al usuario IAM que proporciona permisos a Cloud Manager.

   La siguiente directiva proporciona los permisos que Cloud Manager necesita para utilizar CMK desde la cuenta de AWS externa. Asegúrese de modificar la región y el ID de cuenta en las secciones "Recursos".

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Para obtener más información sobre este proceso, consulte "Documentación de AWS: Permitir que las cuentas de AWS externas puedan acceder a un CMK".

Requisitos de red

Requisitos de red para Cloud Manager

Configure su red para que Cloud Manager pueda poner en marcha sistemas de Cloud Volumes ONTAP en AWS, Microsoft Azure o Google Cloud Platform. El paso más importante es garantizar el acceso saliente a Internet a varios puntos finales.

Si la red utiliza un servidor proxy para toda la comunicación a Internet, Cloud Manager le solicita que especifique el proxy durante la instalación. También puede especificar el servidor proxy en la página Configuración. Consulte "Configuración de Cloud Manager para usar un servidor proxy".

Conexión a redes de destino

Cloud Manager requiere una conexión de red a los VPC y VNets en los que desea implementar Cloud Volumes ONTAP.

Por ejemplo, si instala Cloud Manager en su red corporativa, debe configurar una conexión VPN al VPC o a vnet en el que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

Cloud Manager requiere acceso a Internet de salida para poner en marcha y gestionar Cloud Volumes ONTAP. También es necesario acceder a Internet de salida al acceder a Cloud Manager desde el explorador web y al ejecutar el instalador de Cloud Manager en un host Linux.

En las siguientes secciones se identifican los puntos finales específicos.

Extremos para gestionar Cloud Volumes ONTAP en AWS

Cloud Manager requiere acceso saliente a Internet para contactar con los siguientes extremos al implementar y gestionar Cloud Volumes ONTAP en AWS:

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3) El extremo exacto depende de la región en la que se implemente Cloud Volumes ONTAP. "Consulte la documentación de AWS para obtener más detalles."	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en AWS.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.

Puntos finales	Específico
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Se utiliza para añadir su ID de cuenta de AWS a la lista de usuarios permitidos para Backup en S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Extremos para gestionar Cloud Volumes ONTAP en Azure

Cloud Manager requiere acceso saliente a Internet para contactar con los siguientes extremos al poner en marcha y gestionar Cloud Volumes ONTAP en Microsoft Azure:

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en la mayoría de las regiones de Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en las regiones de Azure Alemania.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permite a Cloud Manager implementar y gestionar Cloud Volumes ONTAP en las regiones de Azure US Gov.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://mysupport.netapp.com	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Extremos para gestionar Cloud Volumes ONTAP en GCP

Cloud Manager requiere acceso saliente a Internet para contactar con los siguientes extremos cuando se pone en marcha y se gestiona Cloud Volumes ONTAP en GCP:

Puntos finales	Específico
https://www.googleapis.com	Permite que Cloud Manager se ponga en contacto con las API de Google para poner en marcha y gestionar Cloud Volumes ONTAP en GCP.
https://api.services.cloud.netapp.com:443	Solicitudes de API a Cloud Central de NetApp.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Proporciona acceso a imágenes, manifiestos y plantillas de software.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com	Permite a Cloud Manager acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
https://kinesis.us-east-1.amazonaws.com	Permite a NetApp transmitir datos desde registros de auditoría.
https://cloudmanager.cloud.netapp.com	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
https://netapp-cloud-account.auth0.com	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
https://mysupport.netapp.com	Comunicación con AutoSupport de NetApp.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
https://ipa-signer.cloudmanager.netapp.com	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
Diversas ubicaciones de terceros, por ejemplo: • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

Puntos finales a los que se accede desde su navegador web

Los usuarios deben acceder a Cloud Manager desde un explorador web. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales:

Puntos finales	Específico
El host de Cloud Manager	Debe introducir la dirección IP del host desde un explorador web para cargar la consola de Cloud Manager. Según su conectividad con el proveedor de cloud, puede usar la IP privada o una IP pública asignada al host: • Una IP privada funciona si dispone de una VPN y. acceso directo a la red virtual • Una IP pública funciona en cualquier situación de red En cualquier caso, debe proteger el acceso a la red garantizando que las reglas de grupo de seguridad permiten el acceso sólo desde IP o subredes autorizadas.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Extremos para instalar Cloud Manager en un host Linux

El instalador de Cloud Manager debe acceder a las siguientes direcciones URL durante el proceso de instalación:

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

Puertos y grupos de seguridad

- Si implementa Cloud Manager desde Cloud Central o desde imágenes de mercado, consulte lo siguiente:
  - "Reglas de grupo de seguridad para Cloud Manager en AWS"
  - "Reglas de grupo de seguridad para Cloud Manager en Azure"
  - "Reglas de firewall para Cloud Manager en GCP"
- Si instala Cloud Manager en un host Linux existente, consulte "Requisitos del host de Cloud Manager".

Requisitos de red para Cloud Volumes ONTAP en AWS

Configurar las redes de AWS para que los sistemas Cloud Volumes ONTAP funcionen correctamente.

Requisitos generales de la red de AWS para Cloud Volumes ONTAP

Los siguientes requisitos deben satisfacerse en AWS.

Acceso a Internet saliente para nodos Cloud Volumes ONTAP

Los nodos Cloud Volumes ONTAP requieren acceso saliente a Internet para enviar mensajes a NetApp AutoSupport, que supervisa proactivamente el estado del almacenamiento.

Las políticas de enrutamiento y firewall deben permitir el tráfico HTTP/HTTPS de AWS a los siguientes extremos para que Cloud Volumes ONTAP pueda enviar mensajes de AutoSupport:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

  Si tiene una instancia NAT, debe definir una regla de grupo de seguridad entrante que permita el tráfico HTTPS desde la subred privada hasta Internet.

Acceso saliente a Internet para el mediador de alta disponibilidad

La instancia del mediador de alta disponibilidad debe tener una conexión saliente al servicio EC2 de AWS para que pueda ayudar a recuperarse de la recuperación tras fallos del almacenamiento. Para proporcionar la conexión, puede agregar una dirección IP pública, especificar un servidor proxy o utilizar una opción manual.

La opción manual puede ser una puerta de enlace NAT o un extremo de la interfaz VPC desde la subred de destino al servicio AWS EC2. Para obtener más detalles sobre los extremos VPC, consulte "Documentación de AWS: Extremos de VPC de la interfaz (AWS PrivateLink)".

Número de direcciones IP

Cloud Manager asigna el siguiente número de direcciones IP a Cloud Volumes ONTAP en AWS:

- Nodo único: Direcciones IP de 6
- Pares DE ALTA DISPONIBILIDAD en AZs individuales: 15 direcciones
- Pares DE ALTA DISPONIBILIDAD en varios AZs: Direcciones IP 15 o 16

  Tenga en cuenta que Cloud Manager crea un LIF de gestión de SVM en sistemas de un solo nodo, pero no en pares de alta disponibilidad en una única zona de disponibilidad. Puede elegir si desea crear una LIF de gestión de SVM en parejas de alta disponibilidad en múltiples AZs.

Una LIF es una dirección IP asociada con un puerto físico. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

Grupos de seguridad

No necesita crear grupos de seguridad porque Cloud Manager lo hace por usted. Si necesita utilizar el suyo propio, consulte "Reglas de grupo de seguridad".

Conexión de Cloud Volumes ONTAP a AWS S3 para los datos organización en niveles

Si desea usar EBS como nivel de rendimiento y AWS S3 como nivel de capacidad, debe asegurarse de que Cloud Volumes ONTAP tenga una conexión con S3. La mejor forma de proporcionar esa conexión es crear un extremo de VPC con el servicio S3. Para ver instrucciones, consulte "Documentación de AWS: Crear un extremo de puerta de enlace".

Al crear el extremo VPC, asegúrese de seleccionar la región, VPC y tabla de rutas que correspondan a la instancia de Cloud Volumes ONTAP. También debe modificar el grupo de seguridad para añadir una regla de HTTPS de salida que habilite el tráfico hacia el extremo de S3. De lo contrario, Cloud Volumes ONTAP no puede conectarse con el servicio S3.

Si experimenta algún problema, consulte "Centro de conocimientos de soporte de AWS: ¿por qué no puedo conectarme a un bloque de S3 mediante un extremo de VPC de puerta de enlace?"

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en AWS y sistemas ONTAP en otras redes, debe tener una conexión VPN entre el VPC de AWS y la otra red, por ejemplo, un vnet de Azure o una red corporativa. Para ver instrucciones, consulte "Documentación de AWS: Configuración de una conexión VPN de AWS".

DNS y Active Directory para CIFS

Si desea aprovisionar almacenamiento CIFS, debe configurar DNS y Active Directory en AWS o ampliar la configuración de sus instalaciones a AWS.

El servidor DNS debe proporcionar servicios de resolución de nombres para el entorno de Active Directory. Puede configurar los conjuntos de opciones DHCP para que utilicen el servidor DNS EC2 predeterminado, que no debe ser el servidor DNS utilizado por el entorno de Active Directory.

Para obtener instrucciones, consulte "Documentación de AWS: Active Directory Domain Services en AWS Cloud: Implementación de referencia de inicio rápido".

Requisitos de red de AWS para alta disponibilidad de Cloud Volumes ONTAP en múltiples AZS

Los requisitos de red adicionales de AWS se aplican a configuraciones de alta disponibilidad de Cloud Volumes ONTAP que utilizan varias zonas de disponibilidad (AZs). Debe revisar estos requisitos antes de iniciar una pareja de ha porque debe introducir los detalles de redes en Cloud Manager.

Para comprender cómo funcionan los pares de alta disponibilidad, consulte "Pares de alta disponibilidad".

Zonas de disponibilidad

Este modelo de puesta en marcha de alta disponibilidad utiliza varios AZs para garantizar una alta disponibilidad de sus datos. Debería utilizar una zona de disponibilidad dedicada para cada instancia de Cloud Volumes ONTAP y la instancia de mediador, que proporciona un canal de comunicación entre el par de alta disponibilidad.

Direcciones IP flotantes para datos de NAS y gestión de clústeres/SVM

Las configuraciones de ALTA DISPONIBILIDAD de varios AZs utilizan direcciones IP flotantes que migran entre nodos en caso de que se produzcan fallos. No se puede acceder a ellos de forma nativa desde fuera del VPC, a menos que usted "Configure una puerta de enlace de tránsito de AWS".

Una dirección IP flotante es para la gestión del clúster, otra para los datos NFS/CIFS del nodo 1 y otra para los datos NFS/CIFS del nodo 2. Una cuarta dirección IP flotante para la gestión de SVM es opcional.

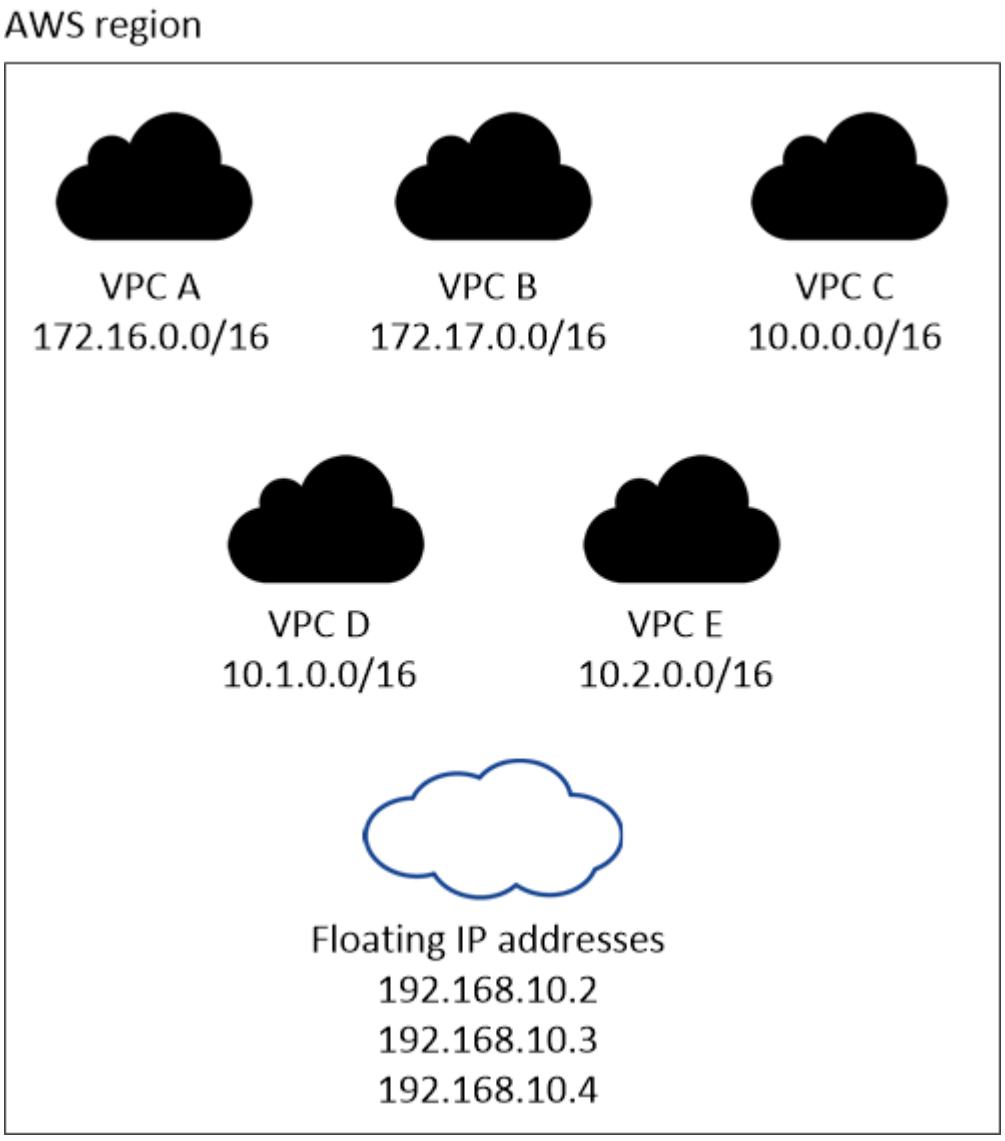
Se requiere una dirección IP flotante para el LIF de gestión de SVM si se usa SnapDrive para Windows o SnapCenter con el par de alta disponibilidad. Si no especifica la dirección IP al implementar el sistema, puede crear la LIF más adelante. Para obtener más información, consulte "Configurar Cloud Volumes ONTAP".

Debe introducir las direcciones IP flotantes en Cloud Manager cuando crea un entorno de trabajo de alta disponibilidad de Cloud Volumes ONTAP. Cloud Manager asigna las direcciones IP a la pareja de alta

disponibilidad cuando arranca el sistema.

Las direcciones IP flotantes deben estar fuera de los bloques CIDR para todas las VPC de la región AWS en la que se implemente la configuración de alta disponibilidad. Piense en las direcciones IP flotantes como una subred lógica que está fuera de las VPC en su región.

En el siguiente ejemplo se muestra la relación entre las direcciones IP flotantes y las VPC en una región de AWS. Mientras las direcciones IP flotantes están fuera de los bloques CIDR para todos los VPC, se pueden enrutar a subredes a través de tablas de ruta.



Cloud Manager crea automáticamente direcciones IP estáticas para el acceso iSCSI y para el acceso NAS desde clientes fuera de VPC. No es necesario cumplir ningún requisito para estos tipos de direcciones IP.

Puerta de enlace de tránsito para habilitar el acceso de IP flotante desde fuera del VPC

"Configure una puerta de enlace de tránsito de AWS" Para habilitar el acceso a las direcciones IP flotantes de una pareja de alta disponibilidad desde fuera del VPC, donde reside el par de alta disponibilidad.

Tablas de rutas

Después de especificar las direcciones IP flotantes en Cloud Manager, debe seleccionar las tablas de rutas que deberían incluir rutas a las direcciones IP flotantes. Esto permite el acceso de los clientes al par de alta disponibilidad.

Si sólo tiene una tabla de rutas para las subredes en el VPC (la tabla de rutas principal), Cloud Manager agrega automáticamente las direcciones IP flotantes a esa tabla de rutas. Si dispone de más de una tabla de rutas, es muy importante seleccionar las tablas de rutas correctas al iniciar el par ha. De lo contrario, es posible que algunos clientes no tengan acceso a Cloud Volumes ONTAP.

Por ejemplo, puede tener dos subredes asociadas a diferentes tablas de rutas. Si selecciona la tabla DE rutas A, pero no la tabla de rutas B, los clientes de la subred asociada a la tabla DE rutas A pueden acceder al par de alta disponibilidad, pero los clientes de la subred asociada a la tabla de rutas B no pueden.

Para obtener más información sobre las tablas de rutas, consulte "Documentación de AWS: Tablas de rutas".

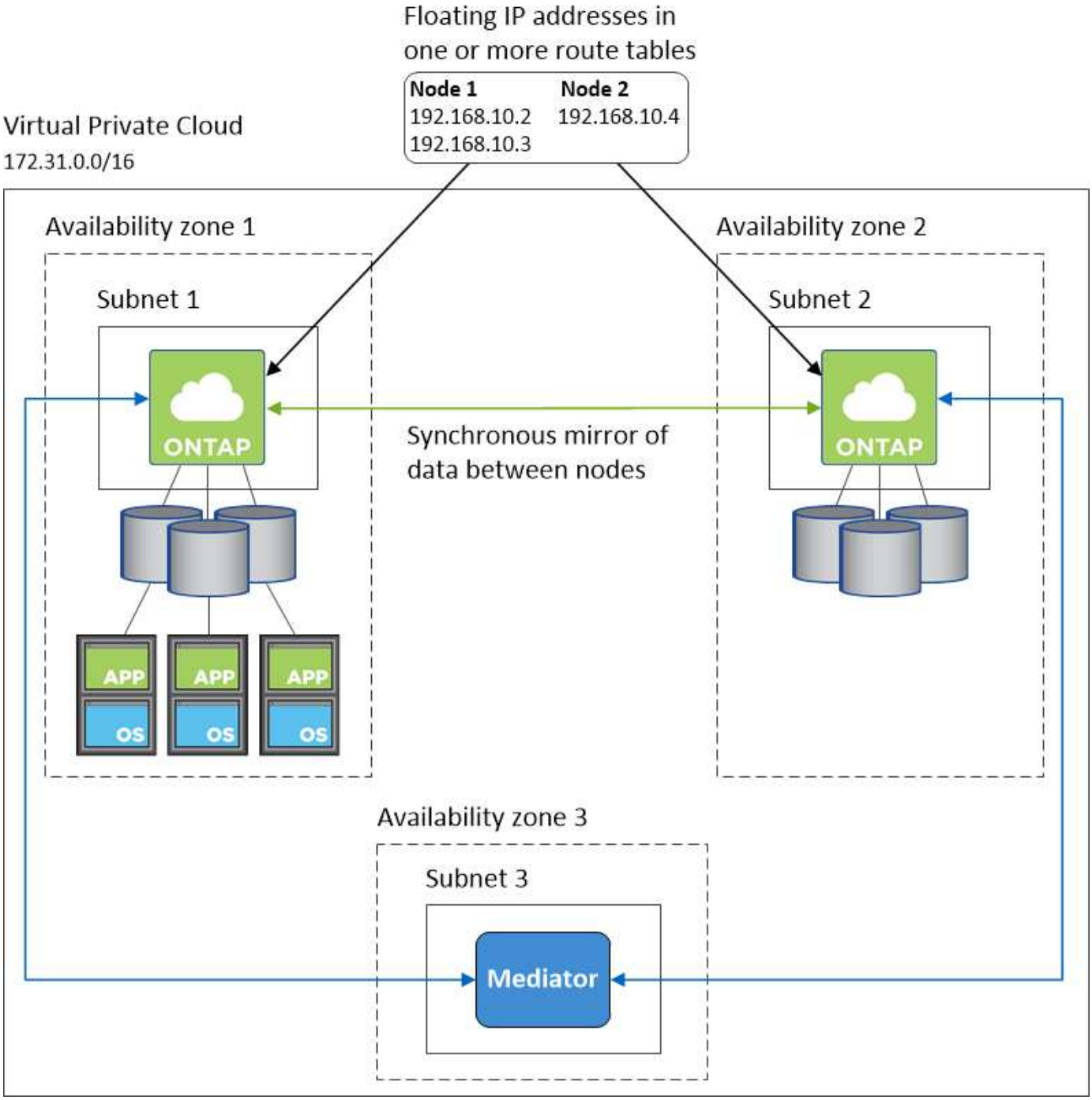
Conexión a herramientas de gestión de NetApp

Para utilizar las herramientas de gestión de NetApp con configuraciones de alta disponibilidad que se encuentran en múltiples AZs, tiene dos opciones de conexión:

1. Puesta en marcha de las herramientas de gestión de NetApp en otro VPC y otras "Configure una puerta de enlace de tránsito de AWS". La puerta de enlace permite el acceso a la dirección IP flotante para la interfaz de gestión del clúster desde fuera del VPC.
2. Ponga en marcha las herramientas de gestión de NetApp en el mismo VPC con una configuración de enrutamiento similar a las de los clientes NAS.

Configuración de ejemplo

En la siguiente imagen, se muestra una configuración de alta disponibilidad óptima en AWS que funciona como una configuración activo-pasivo:



Configuraciones VPC de muestra

Para comprender mejor cómo poner en marcha Cloud Manager y Cloud Volumes ONTAP en AWS, debe revisar las configuraciones más habituales del VPC.

- VPC con subredes públicas y privadas y un dispositivo NAT
- Un VPC con una subred privada y una conexión VPN a la red

VPC con subredes públicas y privadas y un dispositivo NAT

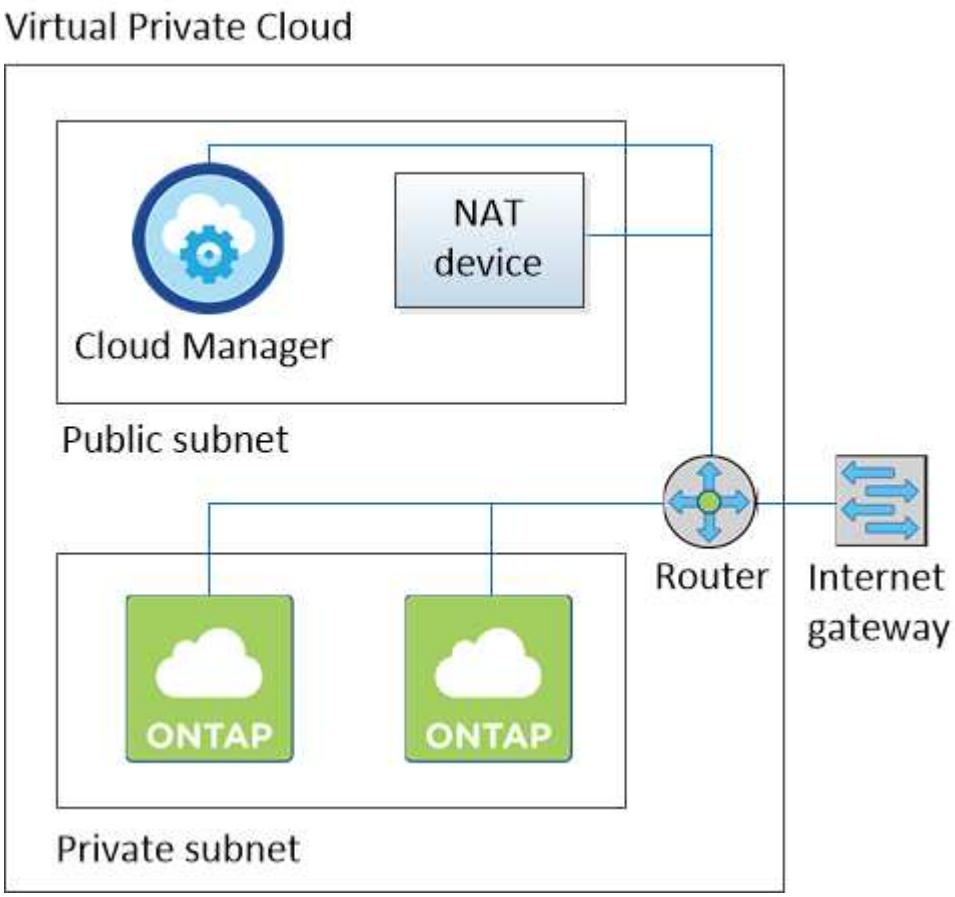
Esta configuración de VPC incluye subredes públicas y privadas, una puerta de enlace de Internet que conecta el VPC a Internet y una instancia de NAT o de NAT en la subred pública que permita el tráfico de

Internet saliente desde la subred privada. En esta configuración, puede ejecutar Cloud Manager en una subred pública o una subred privada, pero se recomienda la subred pública porque permite el acceso de hosts fuera del VPC. A continuación, puede iniciar instancias de Cloud Volumes ONTAP en la subred privada.

> En lugar de un dispositivo NAT, puede utilizar un proxy HTTP para proporcionar conectividad a Internet.

Para obtener más información sobre este escenario, consulte "Documentación de AWS: Escenario 2: VPC con subredes públicas y privadas (NAT)".

En el siguiente gráfico se muestra la ejecución de Cloud Manager en una subred pública y sistemas de solo nodos que se ejecutan en una subred privada:



Un VPC con una subred privada y una conexión VPN a la red

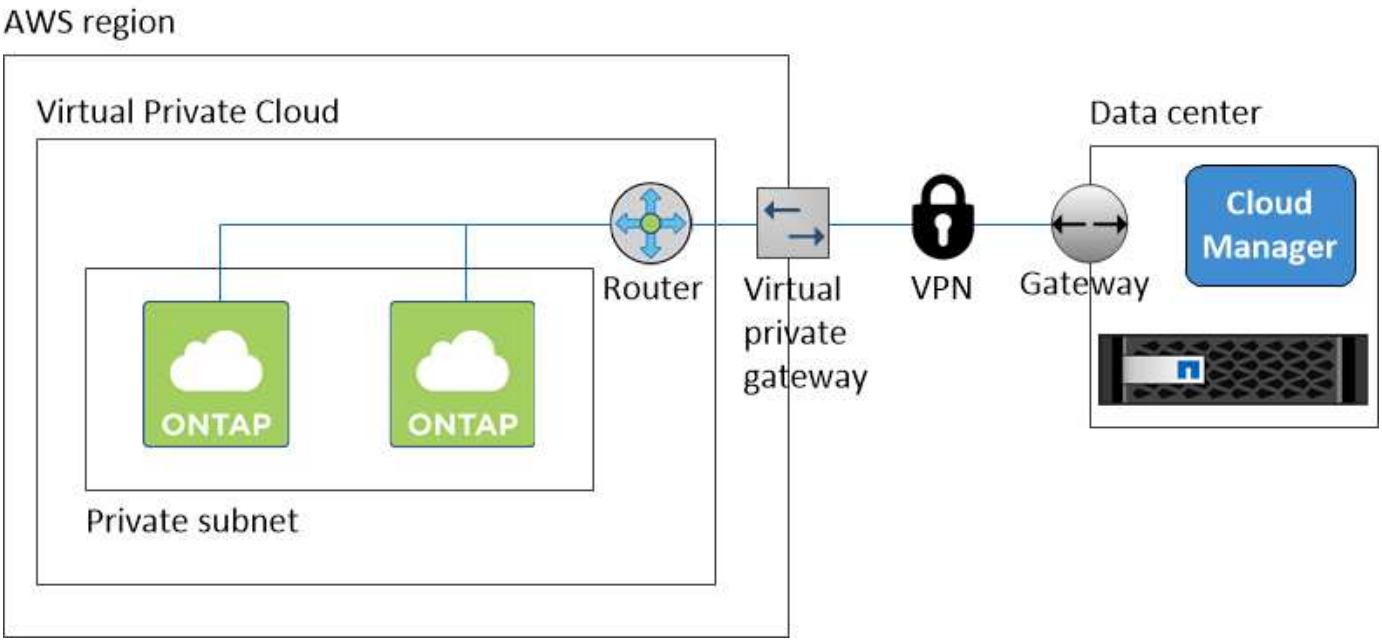
Esta configuración de VPC es una configuración de cloud híbrido en la que Cloud Volumes ONTAP se convierte en una extensión del entorno privado. La configuración incluye una subred privada y una puerta de enlace privada virtual con una conexión VPN a la red. El enrutamiento a través del túnel VPN permite que las instancias EC2 accedan a Internet a través de la red y los firewalls. Puede ejecutar Cloud Manager en la subred privada o en su centro de datos. A continuación, debe iniciar Cloud Volumes ONTAP en la subred privada.

> También puede utilizar un servidor proxy en esta configuración para permitir el acceso a Internet. El servidor proxy puede estar en su centro de datos o en AWS.

Si desea replicar datos entre los sistemas FAS de su centro de datos y los sistemas Cloud Volumes ONTAP de AWS, debe utilizar una conexión VPN para que el enlace sea seguro.

Para obtener más información sobre este escenario, consulte "Documentación de AWS: Escenario 4: VPC con solo una subred privada y acceso de VPN gestionado de AWS".

El siguiente gráfico muestra la ejecución de Cloud Manager en su centro de datos y los sistemas de un solo nodo que se ejecutan en una subred privada:



Configuración de una puerta de enlace de tránsito de AWS para parejas de alta disponibilidad en AZs múltiples

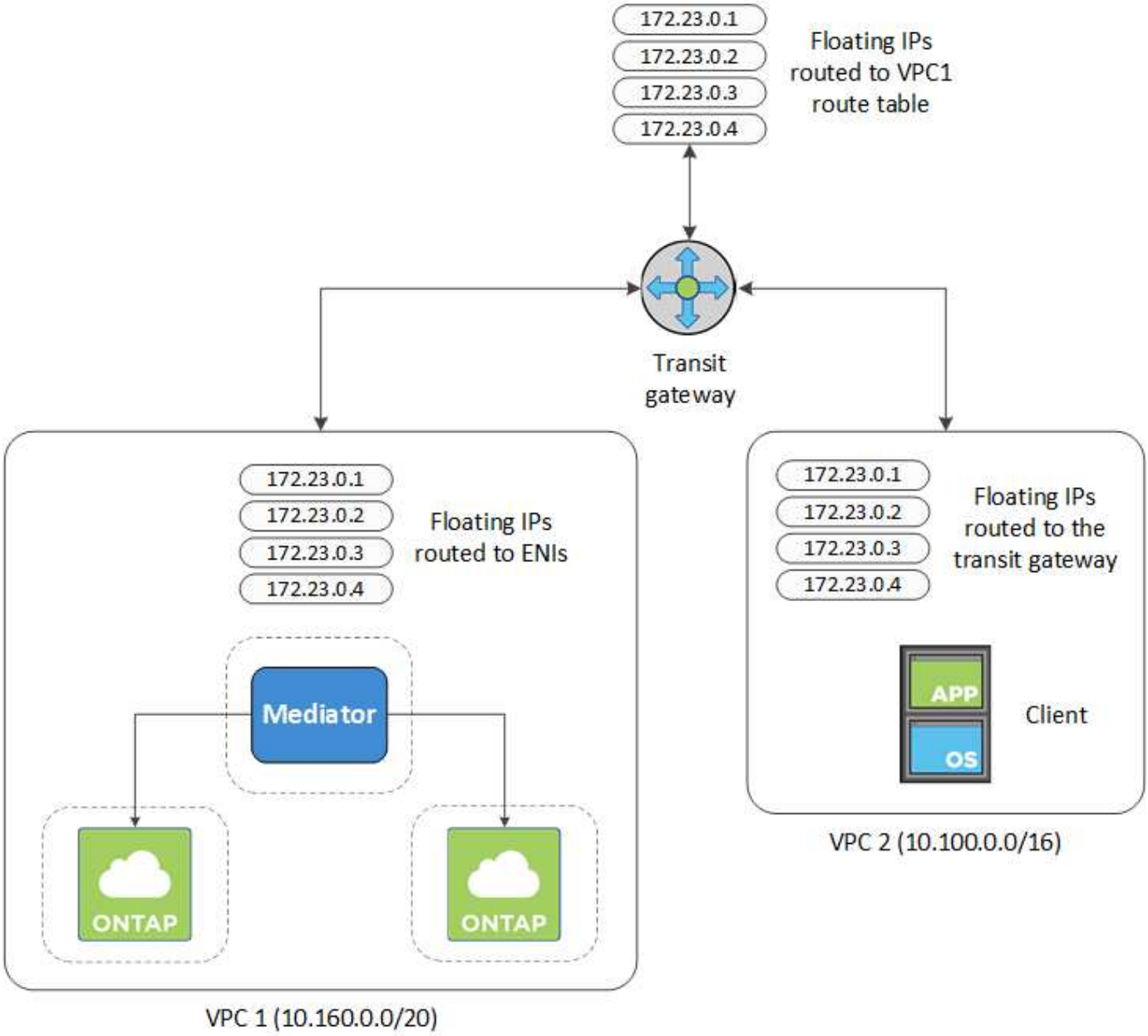
Configure una puerta de enlace de tránsito de AWS para permitir el acceso a las direcciones IP flotantes de un par de alta disponibilidad desde fuera del VPC donde reside el par de alta disponibilidad.

Cuando una configuración de alta disponibilidad de Cloud Volumes ONTAP se distribuye por varias zonas de disponibilidad de AWS, se necesitan direcciones IP flotantes para el acceso a datos de NAS desde el VPC. Estas direcciones IP flotantes pueden migrar entre nodos cuando se producen fallos, pero no están accesibles desde fuera del VPC de forma nativa. Las direcciones IP privadas independientes proporcionan acceso a los datos desde fuera del VPC, pero no proporcionan una recuperación tras fallos automática.

Las direcciones IP flotantes también se requieren para la interfaz de gestión de clústeres y la LIF de gestión de SVM opcional.

Si configura una puerta de enlace de tránsito de AWS, debe habilitar el acceso a las direcciones IP flotantes desde fuera del VPC donde reside el par de alta disponibilidad. Esto significa que los clientes NAS y las herramientas de gestión de NetApp fuera del VPC pueden acceder a las IP flotantes.

Este es un ejemplo que muestra dos VPC conectados por una puerta de enlace de tránsito. Un sistema de alta disponibilidad reside en un VPC, mientras que un cliente reside en el otro. A continuación, podría montar un volumen NAS en el cliente mediante la dirección IP flotante.

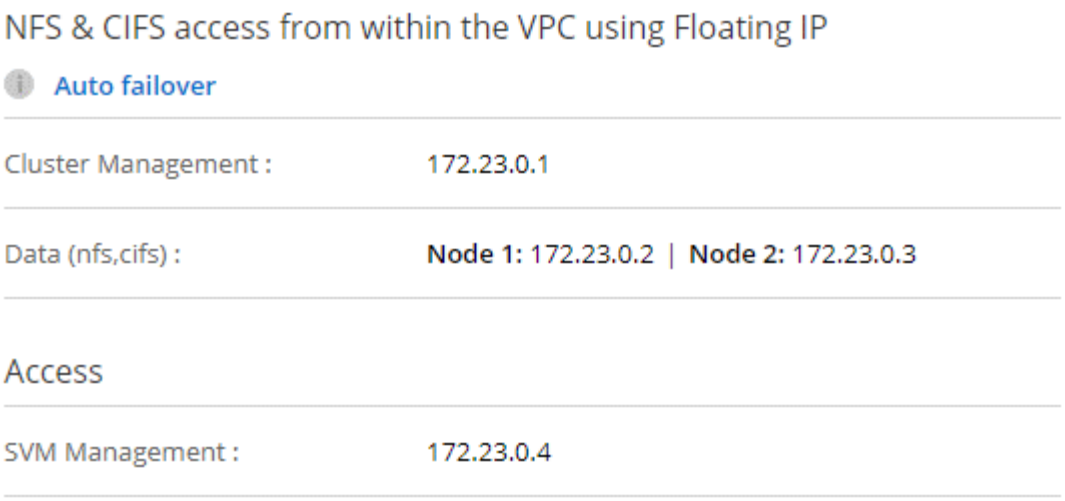


Los siguientes pasos ilustran cómo configurar una configuración similar.

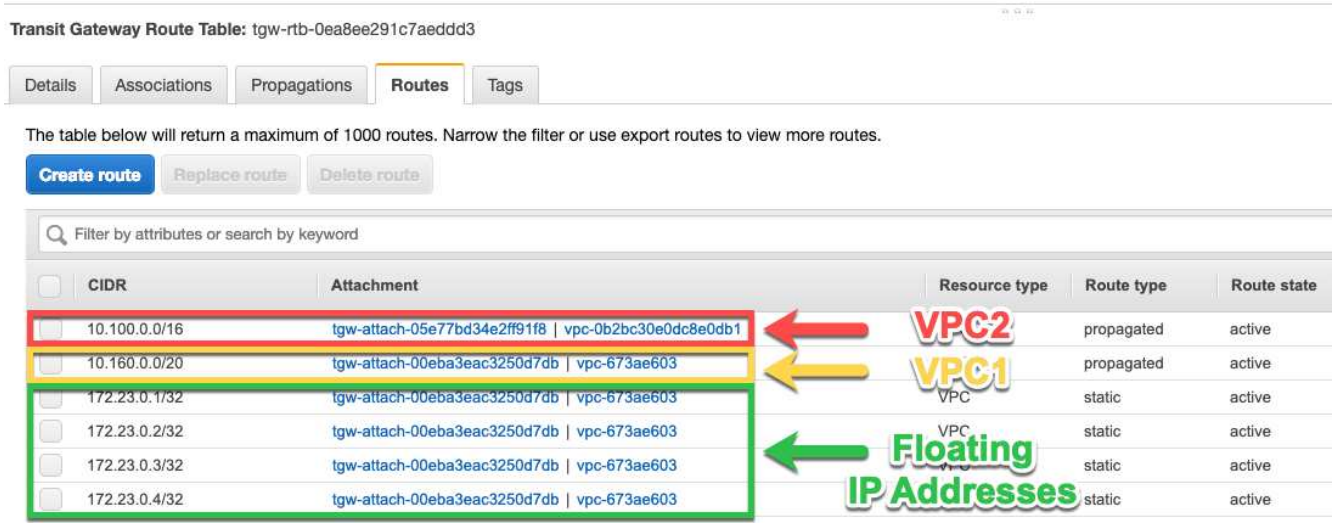
Pasos

1. "Cree una puerta de enlace de tránsito y conecte las VPC al puerta de enlace".
2. Cree rutas en la tabla de rutas de la puerta de enlace de tránsito especificando las direcciones IP flotantes del par de alta disponibilidad.

   Puede encontrar las direcciones IP flotantes en la página Información del entorno de trabajo de Cloud Manager. Veamos un ejemplo:

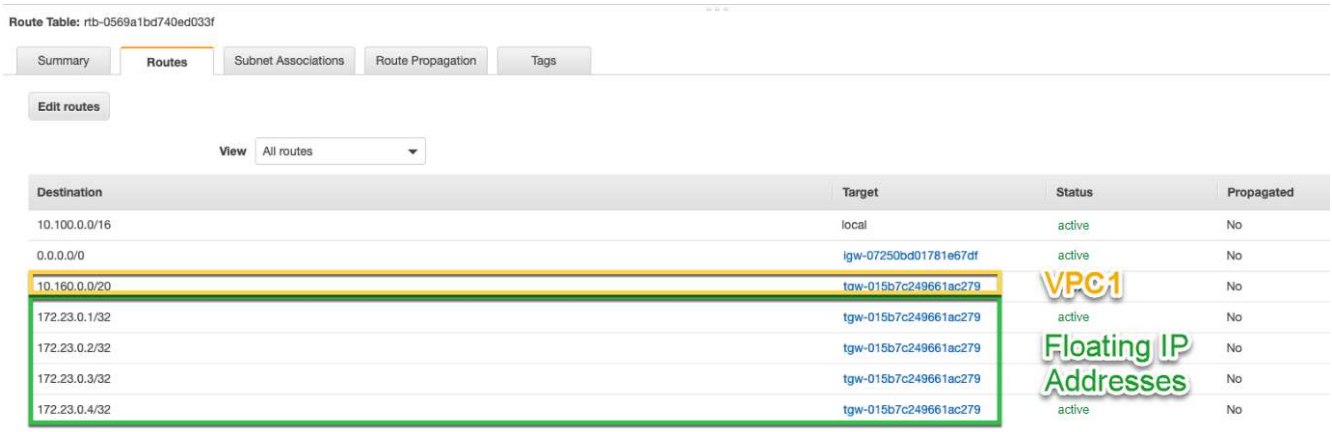


La siguiente imagen de ejemplo muestra la tabla de rutas para la puerta de enlace de tránsito. Incluye rutas a los bloques CIDR de las dos VPC y cuatro direcciones IP flotantes utilizadas por Cloud Volumes ONTAP.



3. Modifique la tabla de rutas de las VPC que necesitan acceder a las direcciones IP flotantes.
   a. Agregar entradas de ruta a las direcciones IP flotantes.
   b. Añada una entrada de ruta al bloque CIDR del VPC donde reside el par de alta disponibilidad.

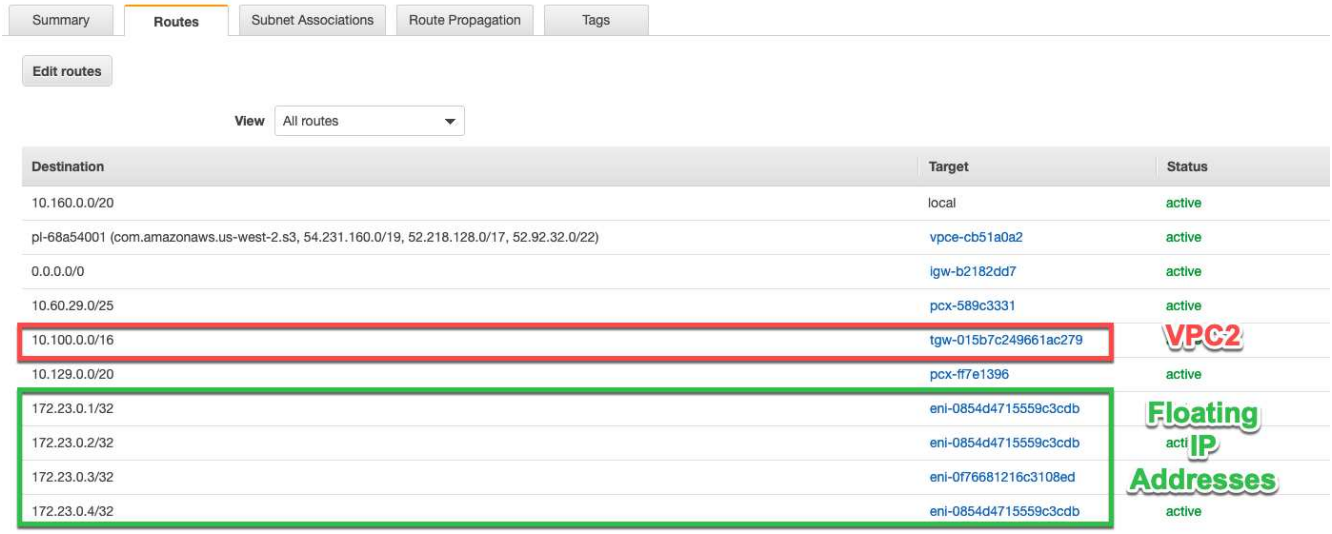
      La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 2, que incluye las rutas hasta VPC 1 y las direcciones IP flotantes.



4. Modifique la tabla de rutas del VPC del par de alta disponibilidad añadiendo una ruta al VPC que necesite acceso a las direcciones IP flotantes.

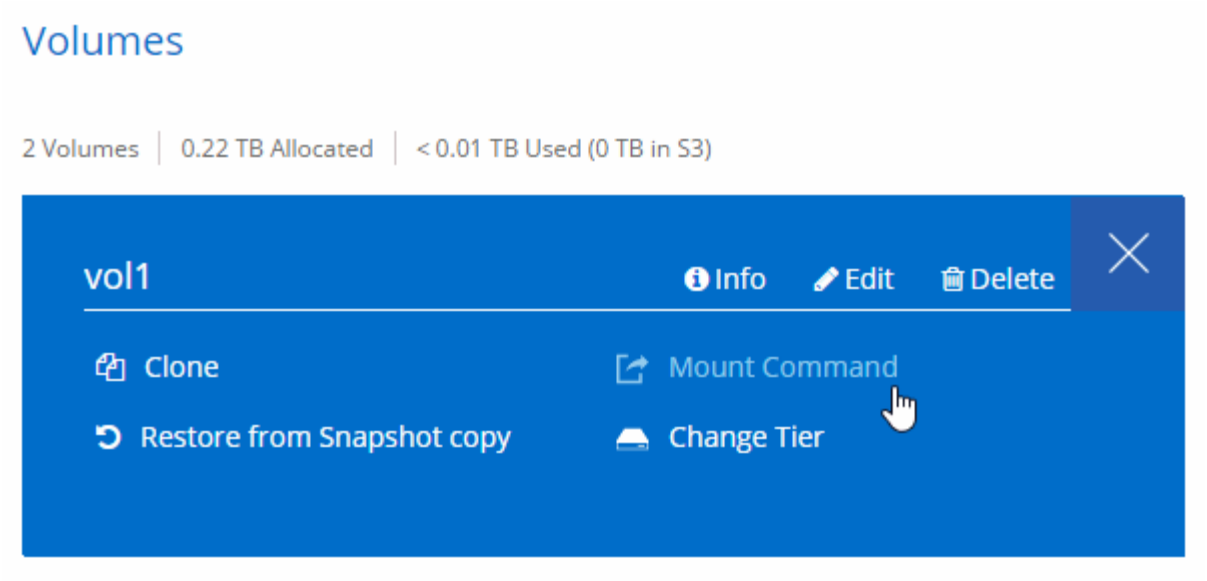
   Este paso es importante porque completa el enrutamiento entre las VPC.

   La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 1. Incluye una ruta a las direcciones IP flotantes y al VPC 2, que es donde reside un cliente. Cloud Manager añadió automáticamente las IP flotantes a la tabla de rutas cuando puso en marcha el par de alta disponibilidad.



5. Montar volúmenes en clientes con la dirección IP flotante.

   Puede encontrar la dirección IP correcta en Cloud Manager seleccionando un volumen y haciendo clic en **Mount Command**.



Enlaces relacionados

- "Pares de alta disponibilidad en AWS"
- "Requisitos de red para Cloud Volumes ONTAP en AWS"

Requisitos de red para Cloud Volumes ONTAP en Azure

Configure sus redes de Azure para que los sistemas Cloud Volumes ONTAP funcionen correctamente.

Acceso saliente a Internet para Cloud Volumes ONTAP

Cloud Volumes ONTAP requiere acceso saliente a Internet para enviar mensajes a NetApp AutoSupport, que supervisa proactivamente el estado del almacenamiento.

Las políticas de enrutamiento y firewall deben permitir el tráfico HTTP/HTTPS a los siguientes extremos para que Cloud Volumes ONTAP pueda enviar mensajes de AutoSupport:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

Grupos de seguridad

No necesita crear grupos de seguridad porque Cloud Manager lo hace por usted. Si necesita utilizar el suyo propio, consulte "Reglas de grupo de seguridad".

Número de direcciones IP

Cloud Manager asigna el siguiente número de direcciones IP a Cloud Volumes ONTAP en Azure:

- Nodo único: Direcciones IP de 5
- Par DE ALTA DISPONIBILIDAD: 16 direcciones IP

  Tenga en cuenta que Cloud Manager crea una LIF de gestión de SVM en parejas de alta disponibilidad, pero no en sistemas de un único nodo en Azure.

Una LIF es una dirección IP asociada con un puerto físico. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

Conexión de Cloud Volumes ONTAP a Azure Blob Storage para organización en niveles de los datos

Si desea organizar en niveles datos fríos en almacenamiento de Azure Blob, no necesita configurar una conexión entre el nivel de rendimiento y el nivel de capacidad mientras Cloud Manager tenga los permisos necesarios Cloud Manager habilita un extremo de servicio vnet para usted si la política de Cloud Manager tiene estos permisos:

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Estos permisos se incluyen en el último "Política de Cloud Manager".

Para obtener más información sobre la configuración de la organización en niveles de datos, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en Azure y sistemas ONTAP en otras redes, debe tener una conexión VPN entre el vnet de Azure y la otra red, por ejemplo, un VPC de AWS o una red de su empresa.

Para obtener instrucciones, consulte "Documentación de Microsoft Azure: Cree una conexión de sitio a sitio en el portal de Azure".

Requisitos de red para Cloud Volumes ONTAP en GCP

Configure sus redes de Google Cloud Platform para que los sistemas Cloud Volumes ONTAP puedan funcionar correctamente.

VPC compartido

Cloud Manager y Cloud Volumes ONTAP son compatibles con un VPC compartido de Google Cloud Platform.

Un VPC compartido permite configurar y gestionar de forma centralizada las redes virtuales de varios proyectos. Puede configurar redes VPC compartidas en el *host project* e implementar las instancias de máquina virtual de Cloud Manager y Cloud Volumes ONTAP en un *service project*. "Documentación de Google Cloud: Información general sobre VPC compartido".

El único requisito es proporcionar los siguientes permisos a la cuenta de servicio de Cloud Manager en el proyecto de host del VPC compartido:

compute.firewalls.* compute.networks.* compute.subredes.*

Cloud Manager necesita estos permisos para consultar los firewalls, VPC y subredes del proyecto de host.

Acceso saliente a Internet para Cloud Volumes ONTAP

Cloud Volumes ONTAP requiere acceso saliente a Internet para enviar mensajes a NetApp AutoSupport, que supervisa proactivamente el estado del almacenamiento.

Las políticas de enrutamiento y firewall deben permitir el tráfico HTTP/HTTPS a los siguientes extremos para que Cloud Volumes ONTAP pueda enviar mensajes de AutoSupport:

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

Número de direcciones IP

Cloud Manager asigna 5 direcciones IP a Cloud Volumes ONTAP en GCP.

Tenga en cuenta que Cloud Manager no crea una LIF de gestión de SVM para Cloud Volumes ONTAP en GCP.

Una LIF es una dirección IP asociada con un puerto físico. Se requiere una LIF de gestión de SVM para herramientas de gestión como SnapCenter.

Reglas del firewall

No necesita crear reglas de firewall, ya que Cloud Manager lo hace por usted. Si necesita utilizar el suyo propio, consulte "Reglas de firewall para GCP".

Conexión de Cloud Volumes ONTAP a Google Cloud Storage para organización en niveles de los datos

Si desea organizar los datos inactivos en niveles en un bucket de Google Cloud Storage, la subred en la que reside Cloud Volumes ONTAP debe estar configurada para Private Google Access. Para obtener instrucciones, consulte "Documentación de Google Cloud: Configuración de Private Google Access".

Si quiere ver los pasos adicionales necesarios para configurar la organización en niveles de los datos en Cloud Manager, consulte "Organización en niveles de los datos inactivos en almacenamiento de objetos de bajo coste".

Conexiones a sistemas ONTAP en otras redes

Para replicar datos entre un sistema Cloud Volumes ONTAP en GCP y los sistemas ONTAP de otras redes, debe tener una conexión VPN entre el VPC y la otra red, por ejemplo, su red corporativa.

Para obtener instrucciones, consulte "Documentación de Google Cloud: Información general sobre Cloud VPN".

Opciones adicionales de puesta en marcha

Requisitos del host de Cloud Manager

Si instala Cloud Manager en su propio host, debe verificar la compatibilidad con su configuración, que incluye requisitos del sistema operativo, de puertos, etc.

Puede instalar Cloud Manager en su propio host en GCP, pero no en la red local. Cloud Manager debe instalarse en GCP para poder poner en marcha Cloud Volumes ONTAP en GCP.

Se requiere un host dedicado

Cloud Manager no es compatible con un host que se comparte con otras aplicaciones. El host debe ser un host dedicado.

Tipos de instancia de AWS EC2 admitidos

- t2.medium
- t3.medium (recomendado)
- m4.grande
- m5.xlarge
- m5,2xgrande
- m5.4xgrande
- m5.8xlarge

Tamaños de máquina virtual de Azure admitidos

A2, D2 v2 o D2 v3 (según disponibilidad)

Tipos de máquinas GCP admitidos

Tipo de máquina con al menos 2 vCPU y 4 GB de memoria.

Sistemas operativos compatibles

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

  El sistema Red Hat Enterprise Linux debe estar registrado con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de terceros necesario durante la instalación de Cloud Manager.

  Cloud Manager es compatible con las versiones en inglés de estos sistemas operativos.

Hipervisor

Un hipervisor de configuración básica o alojado certificado Ejecute CentOS o Red Hat Enterprise Linuxhttps://access.redhat.com/certified-hypervisors["Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"^]

CPU

2.27 GHz o superior con dos núcleos

RAM

4 GB

Libere espacio en disco

50 GB

Acceso a Internet de salida

Se requiere acceso saliente a Internet cuando se instala Cloud Manager y cuando se utiliza Cloud Manager para implementar Cloud Volumes ONTAP. Para ver una lista de extremos, consulte "Requisitos de red para Cloud Manager".

Puertos

Deben estar disponibles los siguientes puertos:

- 80 para acceso HTTP
- 443 para acceso HTTPS
- 3306 para la base de datos de Cloud Manager
- 8080 para el proxy de API de Cloud Manager

Si otros servicios utilizan estos puertos, se produce un error en la instalación de Cloud Manager.

> Existe un posible conflicto con el puerto 3306. Si otra instancia de MySQL se ejecuta en el host, utiliza el puerto 3306 de manera predeterminada. Debe cambiar el puerto que utiliza la instancia de MySQL existente.

Puede cambiar los puertos HTTP y HTTPS predeterminados al instalar Cloud Manager. No puede cambiar el puerto predeterminado para la base de datos MySQL. Si cambia los puertos HTTP y HTTPS, debe asegurarse de que los usuarios puedan acceder a la consola web de Cloud Manager desde un host remoto:

- Modifique el grupo de seguridad para permitir las conexiones entrantes a través de los puertos.
- Especifique el puerto cuando introduzca la URL en la consola web de Cloud Manager.

Instalar Cloud Manager en un host Linux existente

El método más habitual de poner en marcha Cloud Manager es desde Cloud Central o desde el mercado de un proveedor de cloud. Pero tiene la opción de descargar e instalar el software Cloud Manager en un host Linux existente de su red o en la nube.

> Puede instalar Cloud Manager en su propio host en GCP, pero no en la red local. Cloud Manager debe instalarse en GCP para poder poner en marcha Cloud Volumes ONTAP en GCP.

Antes de empezar

- Debe registrarse un sistema Red Hat Enterprise Linux con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software de terceros necesario durante la instalación de Cloud Manager.
- El instalador de Cloud Manager accede a varias URL durante el proceso de instalación. Debe asegurarse de que se permite el acceso saliente a Internet a esos puntos finales. Consulte "Requisitos de red para Cloud Manager".

Acerca de esta tarea

- No se requieren privilegios de usuario raíz para instalar Cloud Manager.
- Cloud Manager instala las herramientas de línea de comandos de AWS (awscli) para habilitar los procedimientos de recuperación del soporte de NetApp.

Si recibe un mensaje que ha fallado al instalar el awscli, puede ignorar el mensaje de forma segura. Cloud Manager puede funcionar correctamente sin las herramientas.

- El instalador disponible en el sitio de soporte de NetApp puede ser una versión anterior. Después de la instalación, Cloud Manager se actualiza automáticamente si hay una nueva versión disponible.

Pasos

1. Revisar los requisitos de red:
   - "Requisitos de red para Cloud Manager"
   - "Requisitos de red para Cloud Volumes ONTAP en AWS"
   - "Requisitos de red para Cloud Volumes ONTAP en Azure"
   - "Requisitos de red para Cloud Volumes ONTAP en GCP"
2. Revisar "Requisitos del host de Cloud Manager".
3. Descargue el software desde la "Sitio de soporte de NetApp"Y, a continuación, cópielo en el host Linux.

   Para obtener ayuda sobre la conexión y copia del archivo en una instancia de EC2 en AWS, consulte "Documentación de AWS: Conexión a la instancia de Linux mediante SSH".

4. Asigne permisos para ejecutar el script.

   ejemplo

   ```
    chmod +x OnCommandCloudManager-V3.7.0.sh
   . Ejecute el script de instalación:
   ```

   ```
   ./OnCommandCloudManager-V3.7.0.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent ejecuta la instalación sin solicitar información.

   Se requiere *proxy* si el host de Cloud Manager está detrás de un servidor proxy.

   proxyport es el puerto del servidor proxy.

   proxyuser es el nombre de usuario del servidor proxy, si se requiere autenticación básica.

   proxypwd es la contraseña del nombre de usuario que ha especificado.

5. A menos que haya especificado el parámetro silent, escriba **y** para continuar la secuencia de comandos y, a continuación, introduzca los puertos HTTP y HTTPS cuando se le solicite.

   Si cambia los puertos HTTP y HTTPS, debe asegurarse de que los usuarios puedan acceder a la consola web de Cloud Manager desde un host remoto:

   - Modifique el grupo de seguridad para permitir las conexiones entrantes a través de los puertos.
   - Especifique el puerto cuando introduzca la URL en la consola web de Cloud Manager.

     Cloud Manager ya está instalado. Al finalizar la instalación, el servicio Cloud Manager (occm) se

reinicia dos veces si especificó un servidor proxy.

6. Abra un explorador web e introduzca la siguiente URL:

   https://ipaddress:port

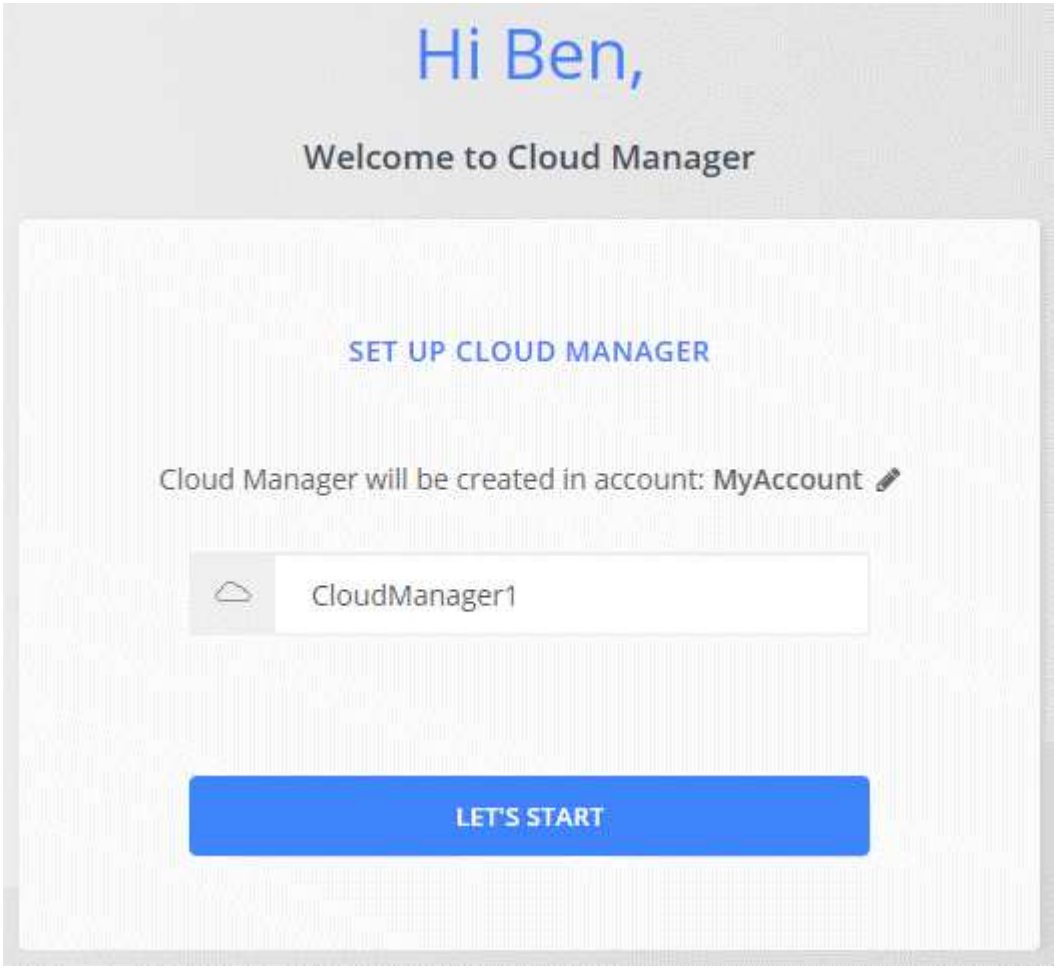
   Ipaddress puede ser localhost, una dirección IP privada o una dirección IP pública, dependiendo de la configuración del host de Cloud Manager. Por ejemplo, si Cloud Manager se encuentra en el cloud público sin una dirección IP pública, debe introducir una dirección IP privada desde un host que tenga una conexión con el host de Cloud Manager.

   Port es obligatorio si cambia los puertos HTTP (80) o HTTPS (443) predeterminados. Por ejemplo, si el puerto HTTPS se ha cambiado a 8443, debe introducir https://ipaddress:8443

7. Regístrese en NetApp Cloud Central o inicie sesión.
8. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con este sistema de Cloud Manager.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Después de terminar

Configure permisos para que Cloud Manager pueda implementar Cloud Volumes ONTAP en su proveedor de cloud:

- AWS: "Configure una cuenta de AWS y, a continuación, añádela Cloud Manager".
- Azure: "Configure una cuenta de Azure y añada a. Cloud Manager".
- GCP: Configure una cuenta de servicio que tenga los permisos que Cloud Manager necesita para crear y gestionar sistemas Cloud Volumes ONTAP en proyectos.
  a. "Crear un rol en GCP" esto incluye los permisos definidos en la "Política de Cloud Manager para GCP".
  b. "Cree una cuenta de servicio de GCP y aplique el rol personalizado que acaba de crear".
  c. "Asocie esta cuenta de servicio a la máquina virtual de Cloud Manager".
  d. Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, "Conceda el acceso añadiendo la cuenta de servicio con la nube La función de gerente de ese proyecto". Deberá repetir este paso con cada proyecto.

Ejecute Cloud Manager desde AWS Marketplace

Se recomienda iniciar Cloud Manager en AWS mediante "Cloud Central de NetApp", Pero puede iniciarlo desde el AWS Marketplace, si es necesario.

Si ejecuta Cloud Manager desde AWS Marketplace, Cloud Manager sigue estando integrado con Cloud Central de NetApp. "Obtenga más información sobre la integración".

Acerca de esta tarea

En los siguientes pasos se describe cómo iniciar la instancia desde la consola de EC2 porque la consola permite asociar un rol IAM a la instancia de Cloud Manager. Esto no es posible usando la acción **Iniciar desde el sitio web**.

Pasos

1. Crear una política de IAM y un rol para la instancia de EC2:
   a. Descargue la política de IAM de Cloud Manager desde la siguiente ubicación:

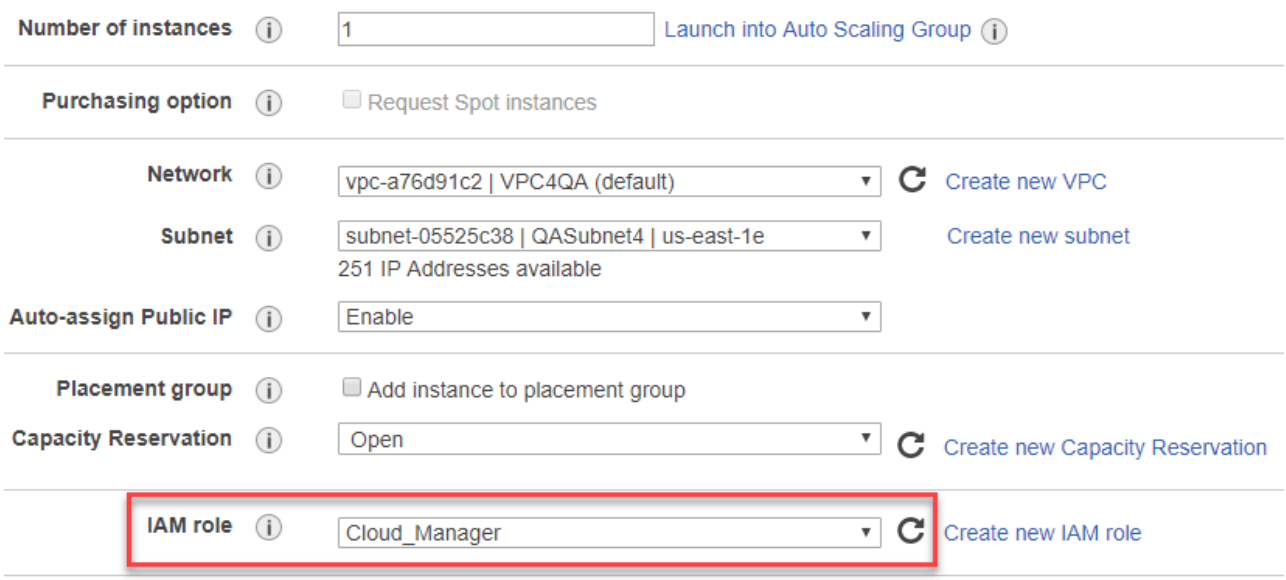
      "NetApp Cloud Manager: Políticas de AWS, Azure y GCP"

   b. Desde la consola de IAM, cree su propia política copiando y pegando el texto de la política IAM de Cloud Manager.
   c. Cree un rol IAM con el tipo de rol Amazon EC2 y asocie la política que ha creado en el paso anterior al rol.
2. "Suscríbase desde el AWS Marketplace" Para garantizar que no se interrumpe el servicio una vez que finaliza la prueba gratuita de Cloud Volumes ONTAP. Se le cobrará de esta suscripción por cada sistema Cloud Volumes ONTAP 9.6 y posterior de PAYGO que cree y cada función complementaria que habilite.
3. Ahora vaya a la "Cloud Manager en el mercado de AWS" Para poner en marcha Cloud Manager desde una AMI.
4. En la página Marketplace, haga clic en **continuar a Suscribirse** y luego haga clic en **continuar a Configuración**.
5. Cambie cualquiera de las opciones predeterminadas y haga clic en **continuar a Iniciar**.
6. En **elegir acción**, seleccione **Iniciar a través de EC2** y, a continuación, haga clic en **Iniciar**.

7. Siga las instrucciones para configurar y desplegar la instancia:
   - **Elegir tipo de instancia**: En función de la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.medium).

     "Revise la lista de tipos de instancia admitidos".

   - **Configurar instancia**: Seleccione un VPC y una subred, la función IAM que creó en el paso 1 y otras opciones de configuración que cumplan sus requisitos.



   - **almacenamiento**: Mantenga las opciones de almacenamiento predeterminadas.
   - **Agregar etiquetas**: Introduzca etiquetas para la instancia, si lo desea.
   - **Configurar grupo de seguridad**: Especifique los métodos de conexión necesarios para la instancia de Cloud Manager: SSH, HTTP y HTTPS.
   - **Revisión**: Revise sus selecciones y haga clic en **Iniciar**.

     AWS inicia el software con la configuración especificada. La instancia y el software de Cloud Manager deben ejecutarse en aproximadamente cinco minutos.

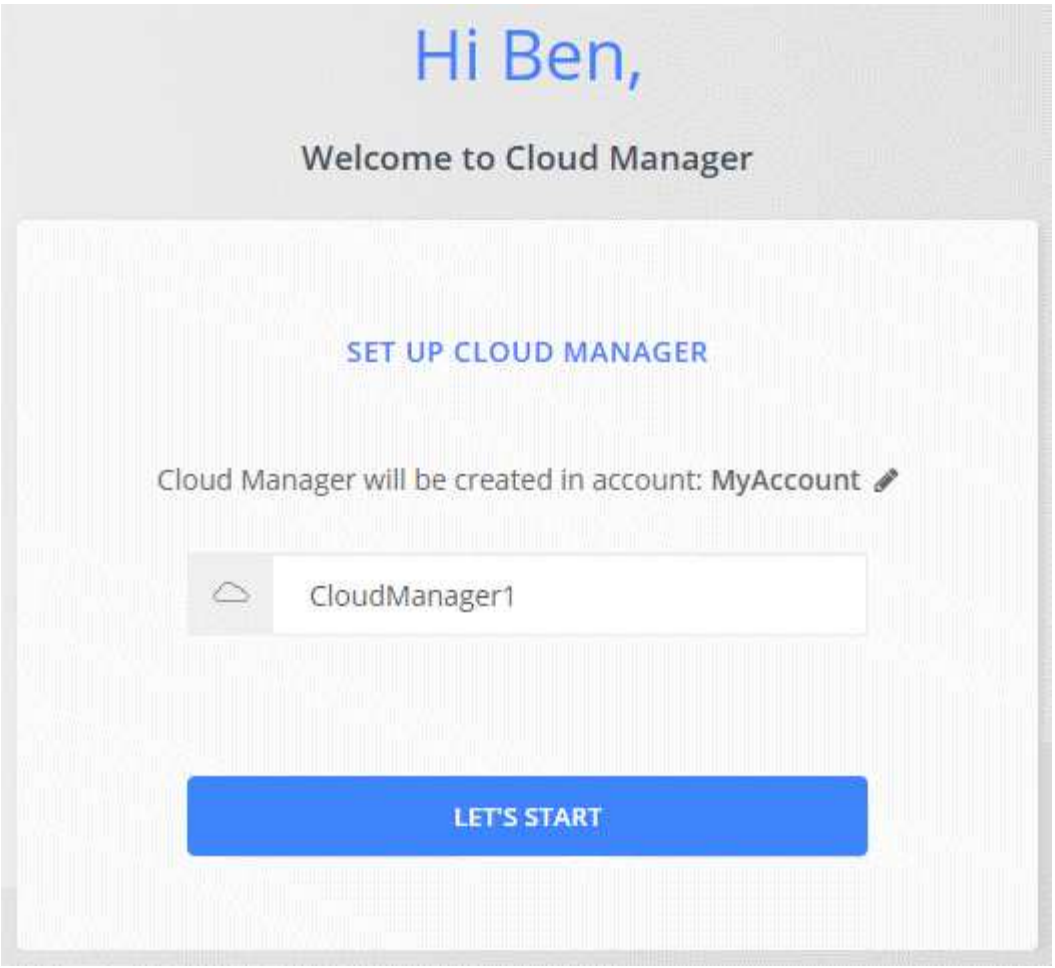
8. Abra un explorador web desde un host que tenga una conexión con la máquina virtual de Cloud Manager e introduzca la siguiente URL:

   http://ipaddress:80

9. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con este sistema de Cloud Manager.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

Cloud Manager ya está instalado y configurado.

Ponga en marcha Cloud Manager desde Azure Marketplace

Se recomienda poner en marcha Cloud Manager en Azure con "Cloud Central de NetApp", Pero puede implementarlo desde Azure Marketplace, si es necesario.

Hay disponibles instrucciones adicionales para implementar Cloud Manager en "Regiones gubernamentales de Azure EE. UU" y en "Regiones de Azure Alemania".

Si pone en marcha Cloud Manager desde Azure Marketplace, Cloud Manager sigue estando integrado con Cloud Central de NetApp. "Obtenga más información sobre la integración".

Implementar Cloud Manager en Azure

Es necesario instalar y configurar Cloud Manager para que pueda usarlo para ejecutar Cloud Volumes ONTAP en Azure.

Pasos

1. "Vaya a la página de Azure Marketplace para Cloud Manager".
2. Haga clic en **Get Now** y, a continuación, haga clic en **Continue**.

3. En el portal de Azure, haga clic en **Crear** y siga los pasos para configurar la máquina virtual.

   Tenga en cuenta lo siguiente al configurar la máquina virtual:

   - Cloud Manager puede ofrecer un rendimiento óptimo tanto con discos HDD como SSD.
   - Elija uno de los tamaños de máquina virtual recomendados: A2, D2 v2 o D2 v3 (según disponibilidad).
   - Para el grupo de seguridad de red, Cloud Manager requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

     "Obtenga más información sobre las reglas de los grupos de seguridad para Cloud Manager".

   - En **Administración**, active **identidad administrada asignada por el sistema** para Cloud Manager seleccionando **On**.

     Esta configuración es importante porque una identidad gestionada permite que la máquina virtual de Cloud Manager se identifique a sí misma en Azure Active Directory sin necesidad de proporcionar credenciales. "Obtenga más información sobre las identidades gestionadas para recursos de Azure".

4. En la página **revisar + crear**, revise las selecciones y haga clic en **Crear** para iniciar la implementación.

   Azure implementa la máquina virtual con los ajustes especificados. La máquina virtual y el software Cloud Manager deben ejecutarse en aproximadamente cinco minutos.

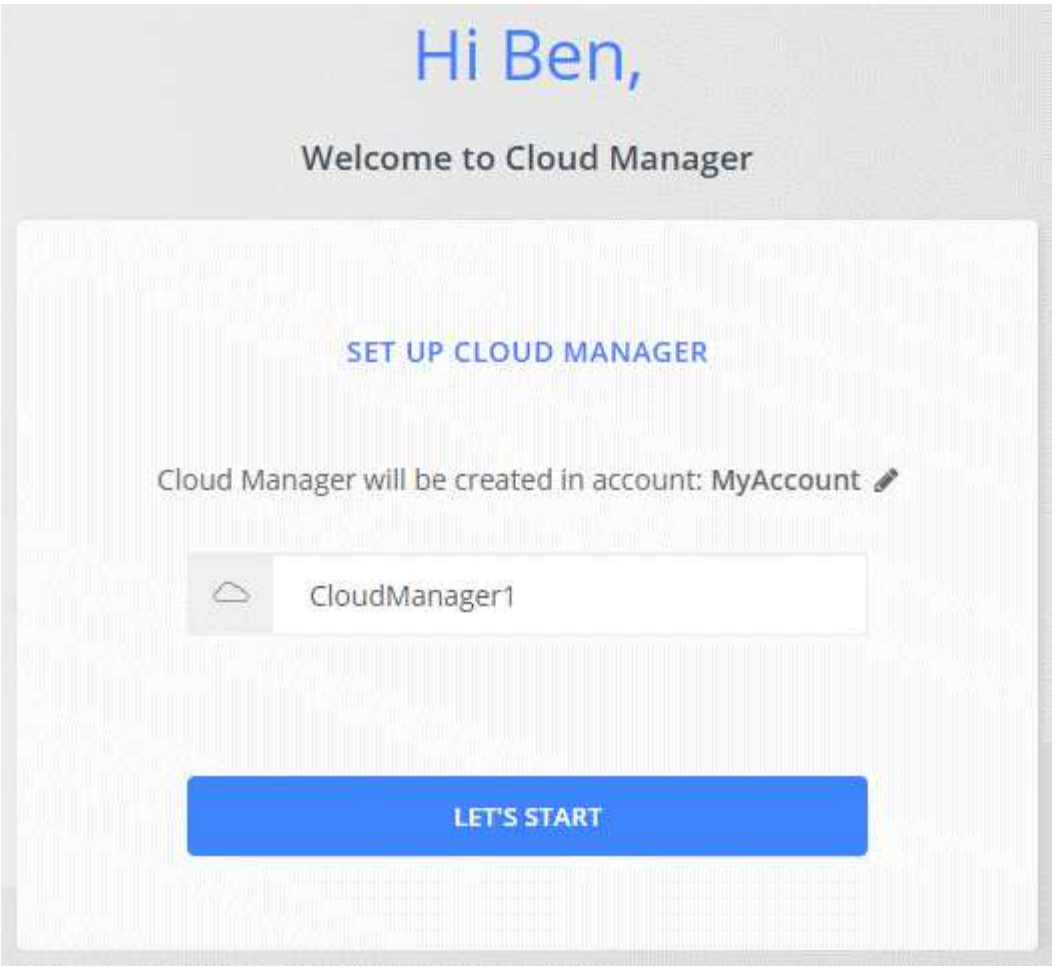
5. Abra un explorador web desde un host que tenga una conexión con la máquina virtual de Cloud Manager e introduzca la siguiente URL:

   http://ipaddress:80

6. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con este sistema de Cloud Manager.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

Cloud Manager ya está instalado y configurado. Debe conceder permisos de Azure para que los usuarios puedan poner en marcha Cloud Volumes ONTAP en Azure.

Otorgando permisos de Azure a Cloud Manager

Al implementar Cloud Manager en Azure, debe haber habilitado un "identidad administrada asignada por el sistema". Ahora debe conceder los permisos de Azure necesarios creando un rol personalizado y, a continuación, asignando el rol a la máquina virtual de Cloud Manager para una o más suscripciones.

Pasos

1. Cree un rol personalizado mediante la política de Cloud Manager:

    a. Descargue el "Política de Azure de Cloud Manager".

    b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

    Debe añadir el ID para cada suscripción de Azure desde la cual los usuarios crearán sistemas Cloud Volumes ONTAP.

    ejemplo

    "AssignableScopes": ["/subscripciones/d333af45-0d07-4154-943d-c25fbzzzzzzz", "/subscripciones/54b91999-b3e6-4599-908e-416e0zzzzzzz", "/subscripciones/398e471c-3bzb6b6b6b3b6bbb3bzb6b6b3b6b3bb6b3b6x-b6b6b3bb

c. Use el archivo JSON para crear una función personalizada en Azure.

   El ejemplo siguiente muestra cómo crear una función personalizada con la CLI de Azure 2.0:

   Az role definition create --role-definition C:\Policy_for_cloud_Manager_Azure_3.7.4.json

Ahora debe tener un rol personalizado llamado operador de Cloud Manager de OnCommand que puede asignar a la máquina virtual de Cloud Manager.

2. Asigne el rol a la máquina virtual de Cloud Manager para una o más suscripciones:
   a. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar sistemas Cloud Volumes ONTAP.
   b. Haga clic en **Control de acceso (IAM)**.
   c. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos:
      - Seleccione el rol **operador de Cloud Manager de OnCommand**.

        El nombre predeterminado que se proporciona en la es el operador de OnCommand Cloud Manager "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

      - Asigne acceso a una **máquina virtual**.
      - Seleccione la suscripción en la que se creó la máquina virtual de Cloud Manager.
      - Seleccione la máquina virtual Cloud Manager.
      - Haga clic en **Guardar**.
   d. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

Resultado

Cloud Manager ahora tiene los permisos que se necesitan para poner en marcha y gestionar Cloud Volumes ONTAP en Azure.

Implementar Cloud Manager en una región gubernamental de Azure Estados Unidos

Para tener Cloud Manager en una región gubernamental de Estados Unidos, ponga en marcha Cloud Manager desde Azure Government Marketplace. A continuación, proporcione los permisos que necesita Cloud Manager para implementar y gestionar sistemas Cloud Volumes ONTAP.

Para obtener una lista de las regiones gubernamentales de EE. UU. De Azure admitidas, consulte "Regiones globales de Cloud Volumes".

Ponga en marcha Cloud Manager desde Azure US Government Marketplace

Cloud Manager está disponible como imagen en el mercado gubernamental de Azure de Estados Unidos.

Pasos

1. Compruebe que Azure Government Marketplace esté habilitado en su suscripción:

a. Inicie sesión en el portal como administrador de empresa.
b. Vaya a **Administrar**.
c. En **Detalles de inscripción**, haga clic en el icono de lápiz junto a **Azure Marketplace**.
d. Seleccione **Activado**.
e. Haga clic en **Guardar**.

"Documentación de Microsoft Azure: Azure Government Marketplace"

2. Busque Cloud Manager de OnCommand en el portal gubernamental de Azure Estados Unidos.
3. Haga clic en **Crear** y siga los pasos para configurar la máquina virtual.

Tenga en cuenta lo siguiente al configurar la máquina virtual:

- Cloud Manager puede ofrecer un rendimiento óptimo tanto con discos HDD como SSD.
- Debe elegir uno de los tamaños de máquina virtual recomendados: A2, D2 v2 o D2 v3 (según disponibilidad).
- Para el grupo de seguridad de red, es mejor elegir **Avanzado**.

  La opción **Avanzado** crea un nuevo grupo de seguridad que incluye las reglas entrantes necesarias para Cloud Manager. Si selecciona básico, consulte "Reglas de grupo de seguridad" para ver la lista de reglas requeridas.

4. En la página de resumen, revise sus selecciones y haga clic en **Crear** para iniciar la implementación.

Azure implementa la máquina virtual con los ajustes especificados. La máquina virtual y el software Cloud Manager deben ejecutarse en aproximadamente cinco minutos.

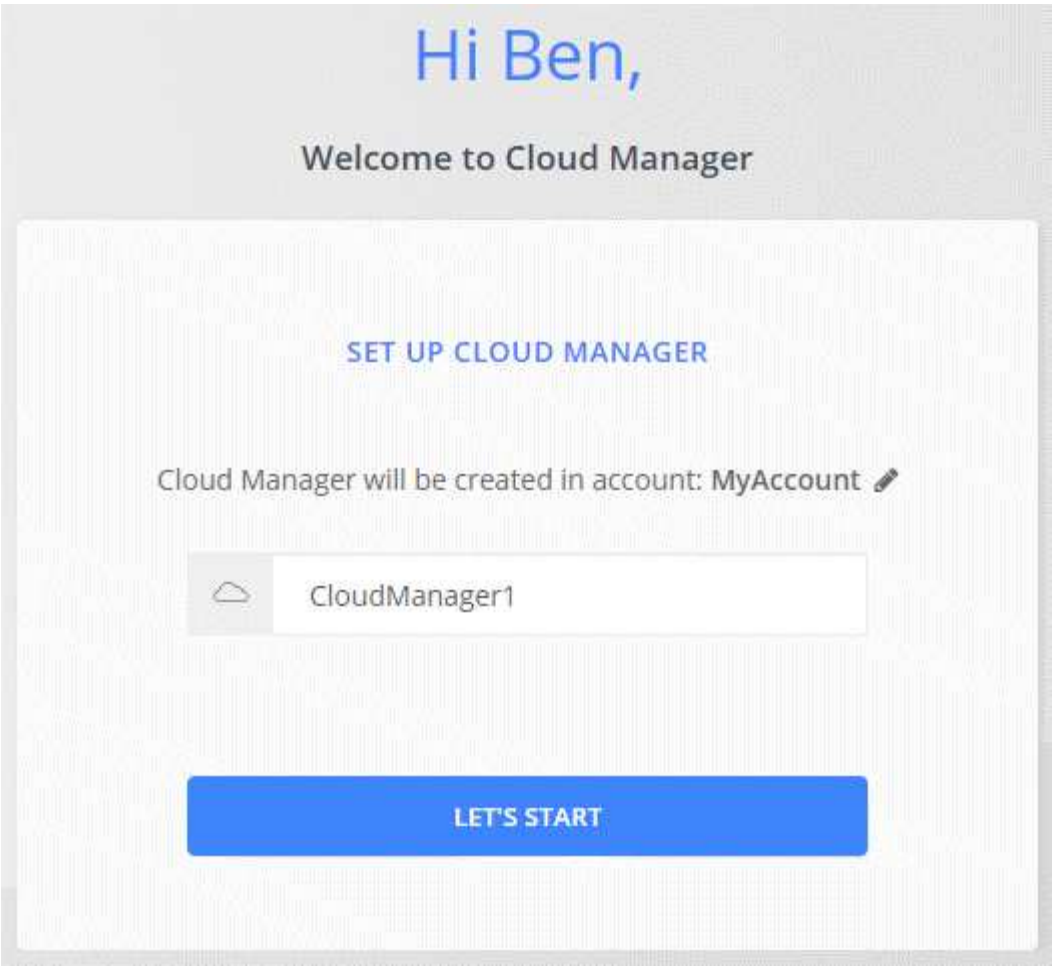
5. Abra un explorador web desde un host que tenga una conexión con la máquina virtual de Cloud Manager e introduzca la siguiente URL:

http://ipaddress:80

6. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con este sistema de Cloud Manager.

      "Obtenga más información acerca de las cuentas de Cloud Central".

   b. Escriba un nombre para el sistema.



Resultado

Cloud Manager ya está instalado y configurado. Debe conceder permisos de Azure para que los usuarios puedan poner en marcha Cloud Volumes ONTAP en Azure.

Concesión de permisos de Azure a Cloud Manager mediante una identidad gestionada

La forma más sencilla de proporcionar permisos consiste en habilitar un "identidad administrada" En la máquina virtual de Cloud Manager, y luego asignando los permisos necesarios a la máquina virtual. Si se prefiere, una forma alternativa es a. "Conceda permisos de Azure con un director de servicio".

Pasos

1. Habilite una identidad administrada en la máquina virtual de Cloud Manager:
   a. Desplácese a la máquina virtual de Cloud Manager y seleccione **identidad**.
   b. En **sistema asignado**, haga clic en **On** y, a continuación, en **Guardar**.
2. Cree un rol personalizado mediante la política de Cloud Manager:
   a. Descargue el "Política de Azure de Cloud Manager".
   b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

      Debe añadir el ID para cada suscripción de Azure desde la cual los usuarios crearán sistemas Cloud Volumes ONTAP.

      ejemplo

"AssignableScopes": ["/subscripciones/d333af45-0d07-4154-943d-c25fbzzzzzzz", "/subscripciones/54b91999-b3e6-4599-908e-416e0zzzzzzz", "/subscripciones/398e471c-3bzb6b6b6b3b6bbb3bzb6b6b3b6b3bb6b3b6x-b6b6b3bb

c. Use el archivo JSON para crear una función personalizada en Azure.

   El ejemplo siguiente muestra cómo crear una función personalizada con la CLI de Azure 2.0:

   Az role definition create --role-definition C:\Policy_for_cloud_Manager_Azure_3.7.4.json

Ahora debe tener un rol personalizado llamado operador de Cloud Manager de OnCommand que puede asignar a la máquina virtual de Cloud Manager.

3. Asigne el rol a la máquina virtual de Cloud Manager para una o más suscripciones:
   a. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar sistemas Cloud Volumes ONTAP.
   b. Haga clic en **Control de acceso (IAM)**.
   c. Haga clic en **Agregar**, haga clic en **Agregar asignación de rol** y, a continuación, agregue los permisos:
      - Seleccione el rol **operador de Cloud Manager de OnCommand**.

        El nombre predeterminado que se proporciona en la es el operador de OnCommand Cloud Manager "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

      - Asigne acceso a una **máquina virtual**.
      - Seleccione la suscripción en la que se creó la máquina virtual de Cloud Manager.
      - Escriba el nombre de la máquina virtual y, a continuación, selecciónelo.
      - Haga clic en **Guardar**.
   d. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

Resultado

Cloud Manager ahora tiene los permisos que se necesitan para poner en marcha y gestionar Cloud Volumes ONTAP en Azure.

Instalando Cloud Manager en una región de Azure Alemania

Azure Marketplace no está disponible en las regiones de Azure Alemania, por lo que debe descargar el instalador de Cloud Manager del sitio de soporte de NetApp e instalarlo en un host Linux existente en la región.

Pasos

1. "Revise los requisitos de red para Azure".
2. "Revise los requisitos del host de Cloud Manager".
3. "Descargue e instale Cloud Manager".
4. "Conceda permisos de Azure a Cloud Manager con un director de servicio".

Después de terminar

Cloud Manager ya está listo para poner en marcha Cloud Volumes ONTAP en la región de Azure Alemania, como en cualquier otra región. Sin embargo, es posible que desee realizar primero la configuración adicional.

Mantener Cloud Manager en funcionamiento

Cloud Manager debe seguir ejecutándose en todo momento.

Cloud Manager es un componente clave en el estado y la facturación de Cloud Volumes ONTAP. Si Cloud Manager se apaga, los sistemas Cloud Volumes ONTAP se apagarán tras perder la comunicación con Cloud Manager durante más de 4 días.