Primeros pasos

Cloud Manager 3.6

NetApp
March 25, 2024

Tabla de contenidos

Primeros pasos

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 de OnCommand.

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
- Cloud de IBM
- En su propia red

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

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

- "Adición de cuentas de proveedor de cloud a Cloud Manager"
- "Instalar un certificado HTTPS"
- "Configurar usuarios e inquilinos"
- "Configuración de AWS KMS"

Puesta en marcha de Cloud Volumes ONTAP

Después de tener Cloud Manager instalado, puede empezar a implementar Cloud Volumes ONTAP en AWS y en Microsoft Azure.

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

- "Configuraciones compatibles para Cloud Volumes ONTAP 9.5"
- "Planificación de la configuración"
- "Inicio de Cloud Volumes ONTAP en AWS"
- "Inicio de Cloud Volumes ONTAP en Azure"

Introducción a Cloud Volumes ONTAP en AWS

Es posible comenzar a usar Cloud Volumes ONTAP en AWS desde NetApp Cloud Central.

1 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 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".

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.

2 Suscríbase a Cloud Volumes ONTAP desde el mercado de AWS

Suscribirse de "El mercado AWS" se requiere para aceptar los términos del software. Sólo debe suscribirse desde el mercado. No es compatible ejecutar Cloud Volumes ONTAP desde cualquier lugar, pero Cloud Manager.

3 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.

4 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".

5 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.

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"
- "Adición de cuentas de proveedor de cloud 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

Es posible comenzar a utilizar Cloud Volumes ONTAP en Azure desde NetApp Cloud Central. Hay disponibles instrucciones adicionales para implementar Cloud Manager en "Regiones gubernamentales de Azure EE. UU" y en "Regiones de Azure Alemania".

1 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".

2 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.

3 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".

4 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 proveedor de cloud a Cloud Manager"
- "Qué hace Cloud Manager con permisos de Azure"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Ejecute Cloud Manager desde Azure Marketplace"

Configurar Cloud Manager

Añadiendo cuentas de proveedores de cloud a Cloud Manager

Si desea poner en marcha Cloud Volumes ONTAP en diferentes cuentas de cloud, debe proporcionar los permisos necesarios para esas cuentas y, a continuación, añadir los detalles a Cloud Manager.

Al implementar Cloud Manager desde Cloud Central, Cloud Manager agrega automáticamente un "cuenta del proveedor de cloud" Para la cuenta en la que implementó Cloud Manager. No se añade una cuenta de proveedor de cloud inicial si instaló manualmente el software Cloud Manager en un sistema existente.

Configurar y añadir cuentas de AWS en Cloud Manager

Si desea poner en marcha Cloud Volumes ONTAP en diferentes cuentas de AWS, tiene que proporcionar los permisos necesarios para esas cuentas y, a continuación, 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.

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

Concesión de permisos al proporcionar 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

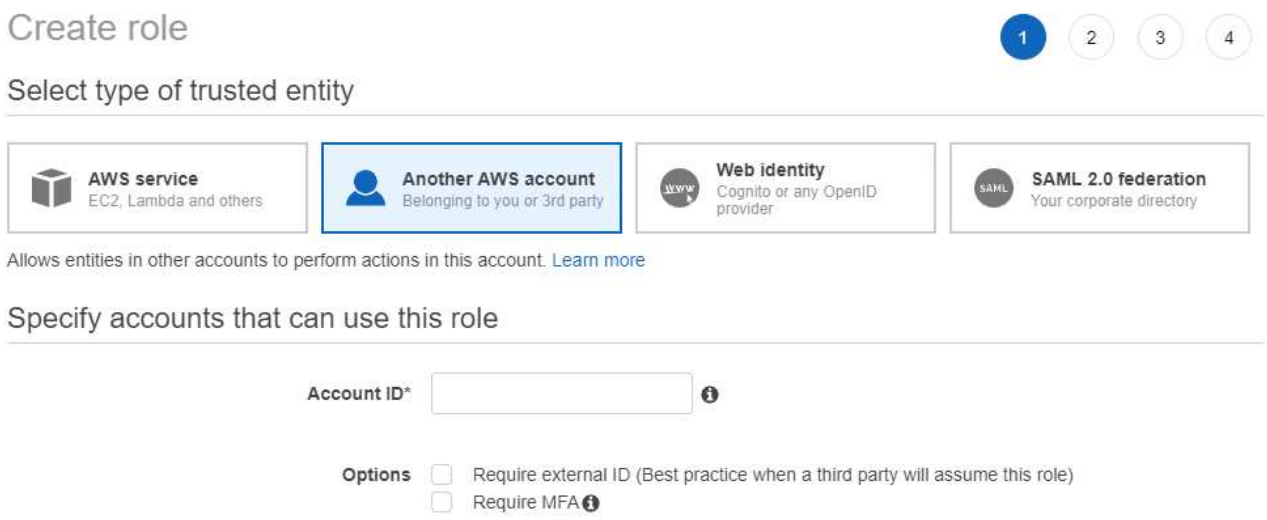
Puede configurar una relación de confianza entre la cuenta de AWS de origen en la que implementó la instancia de Cloud Manager y otras cuentas de AWS mediante los roles de IAM. A continuación, debe proporcionar a Cloud Manager el ARN de las funciones de IAM de las cuentas de confianza.

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

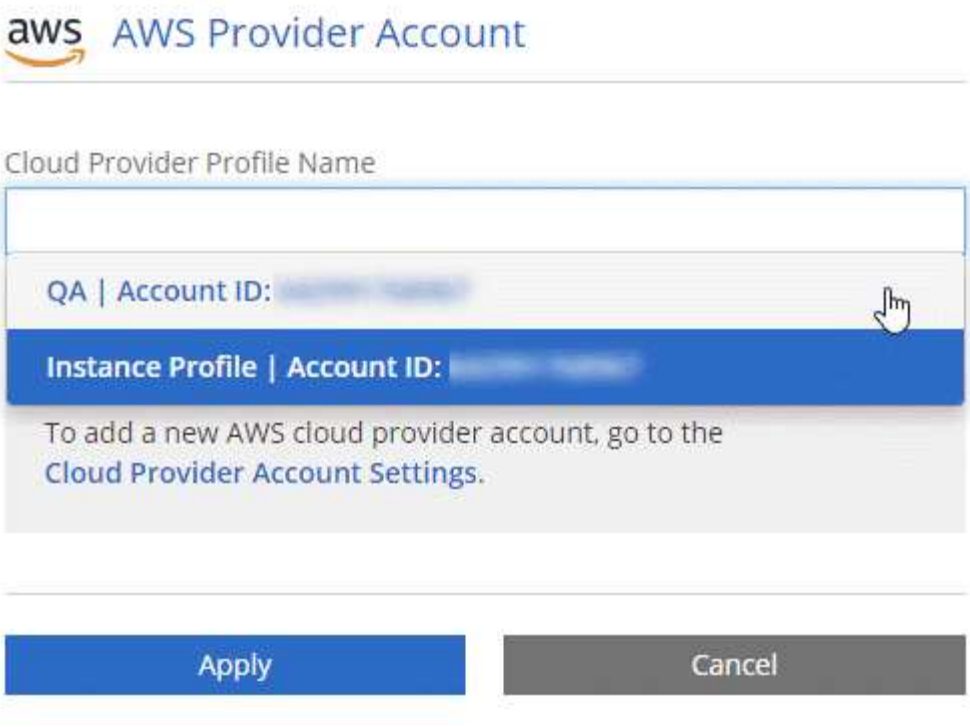
Después de proporcionar una cuenta de AWS con los permisos necesarios, puede añadir la cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en la lista desplegable de tareas y, a continuación, seleccione **Configuración de cuenta**.
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.

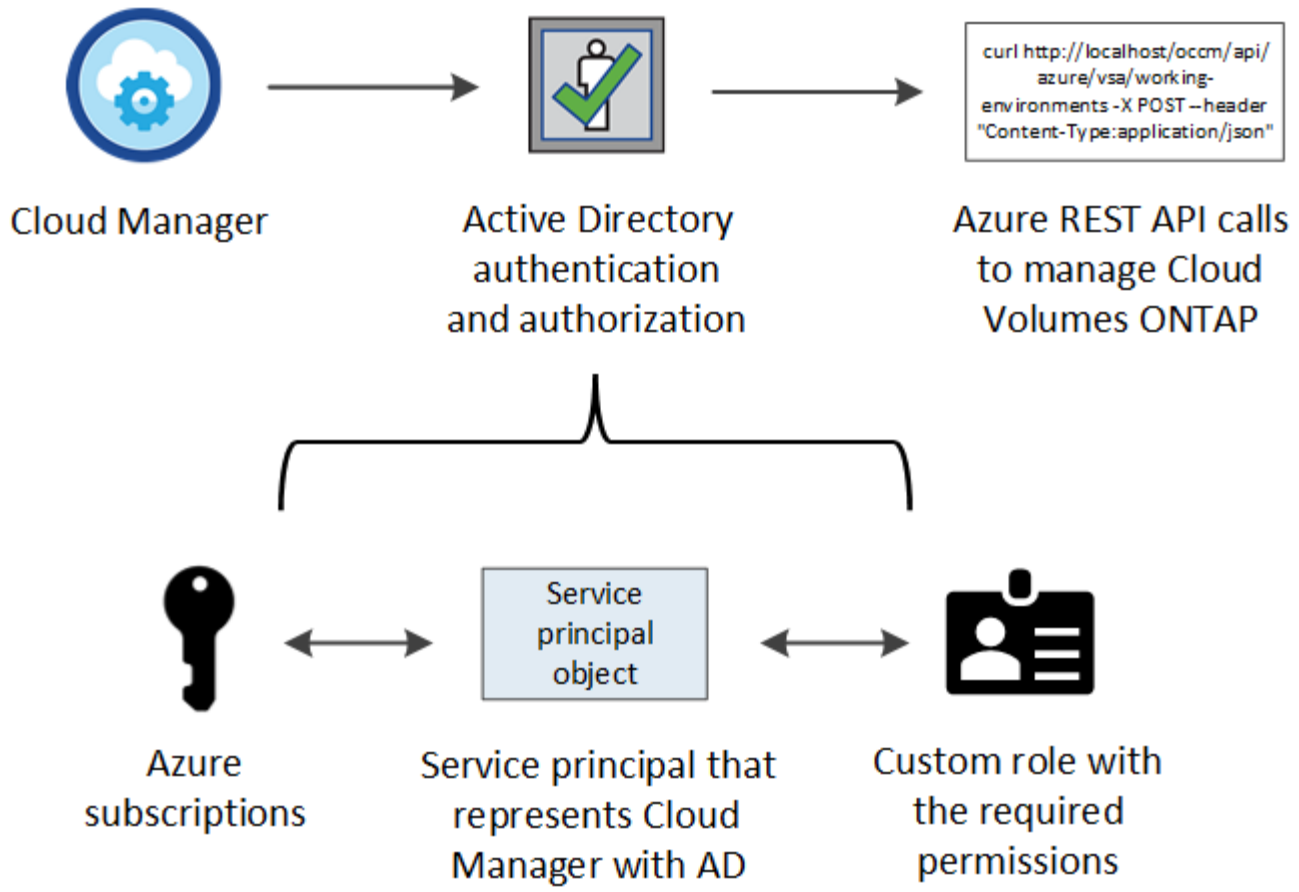
- Concesión de permisos de Azure con un director de servicio
- Adición de cuentas de Azure a Cloud Manager

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.



Los siguientes pasos utilizan el nuevo portal de Azure. Si tiene algún problema, debería utilizar el portal clásico de Azure.

Pasos

1. Cree un rol personalizado con los permisos de Cloud Manager necesarios.
2. Cree un principal de servicio de Active Directory.
3. Asigne el rol de operador personalizado de Cloud Manager al principal de servicio.

Crear un rol personalizado con los permisos de Cloud Manager necesarios

Se requiere un rol personalizado para proporcionar a Cloud Manager los permisos que necesita para iniciar y gestionar Cloud Volumes ONTAP en Azure.

Pasos

1. Descargue el "Política de Azure de Cloud Manager".
2. 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"
```

3. 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_3.6.1.json

Resultado

Ahora debe tener un rol personalizado llamado operador de Cloud Manager de OnCommand.

Creación de una entidad de servicio de Active Directory

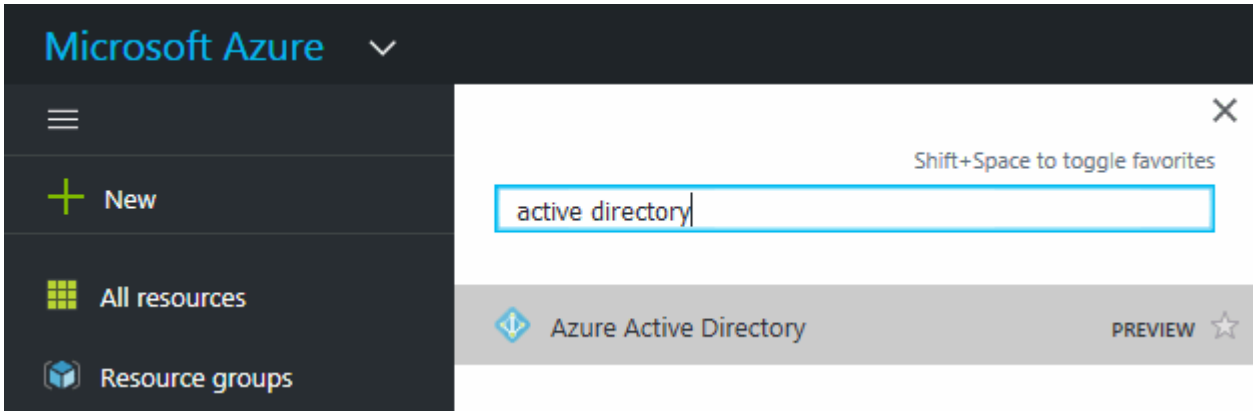
Debe crear un director de servicio de Active Directory para que Cloud Manager se pueda autenticar con Azure Active Directory.

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: Utilice el portal para crear una aplicación de Active Directory y una entidad de servicio con acceso a los recursos".

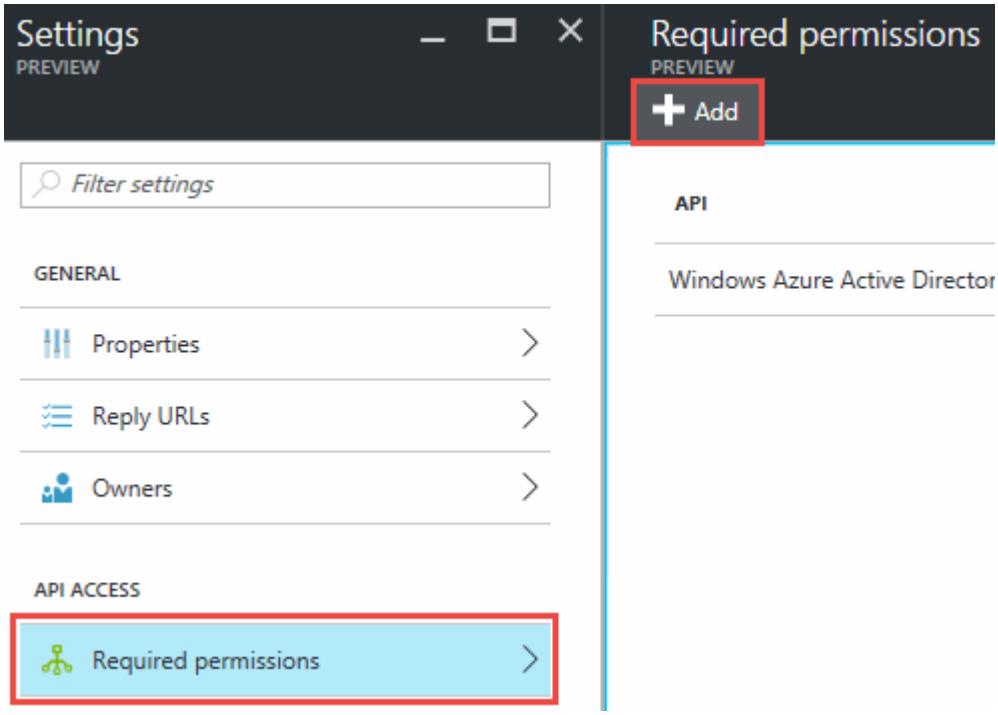
Pasos

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

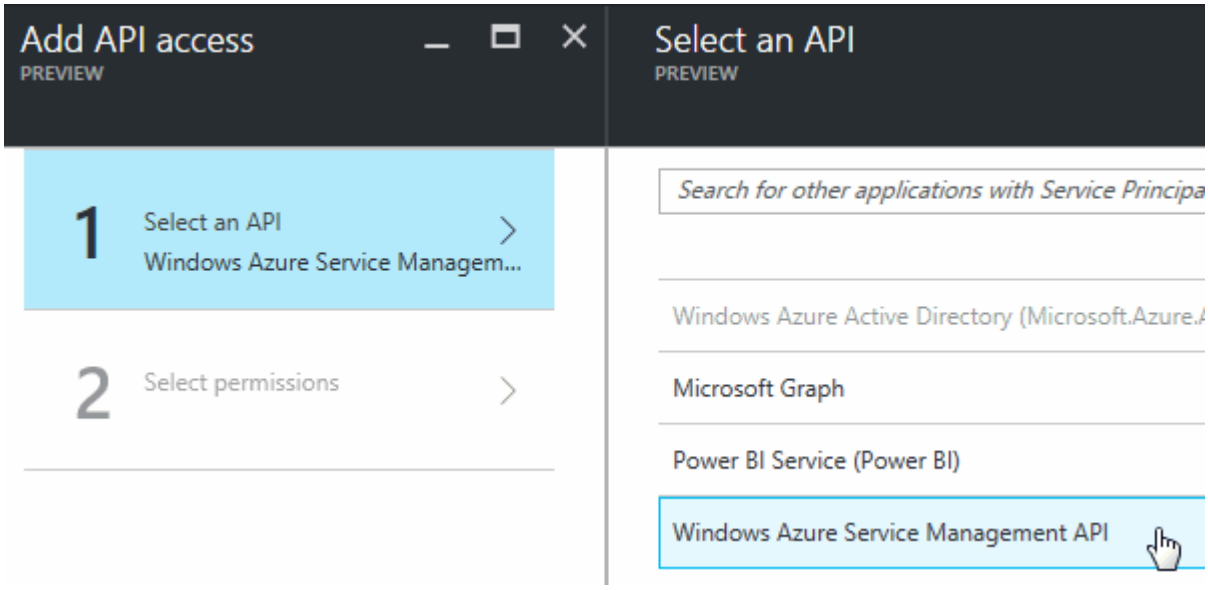


2. En el menú, haga clic en **registros de aplicaciones (Legacy)**.
3. Crear el principal de servicio:
   a. Haga clic en **Nuevo registro de aplicación**.
   b. Introduzca un nombre para la aplicación, mantenga seleccionada **aplicación web / API** y, a continuación, introduzca cualquier URL, por ejemplo, http://url
   c. Haga clic en **Crear**.
4. Modifique la aplicación para agregar los permisos necesarios:
   a. Seleccione la aplicación creada.

b. En Configuración, haga clic en **permisos necesarios** y, a continuación, haga clic en **Agregar**.



c. Haga clic en **Seleccionar una API**, seleccione **Windows Azure Service Management API** y, a continuación, haga clic en **Seleccionar**.



d. Haga clic en **Access Azure Service Management as organization users**, haga clic en **Select** y, a continuación, haga clic en **Done**.

5. Cree una clave para el principal de servicio:

   a. En Configuración, haga clic en **teclas**.

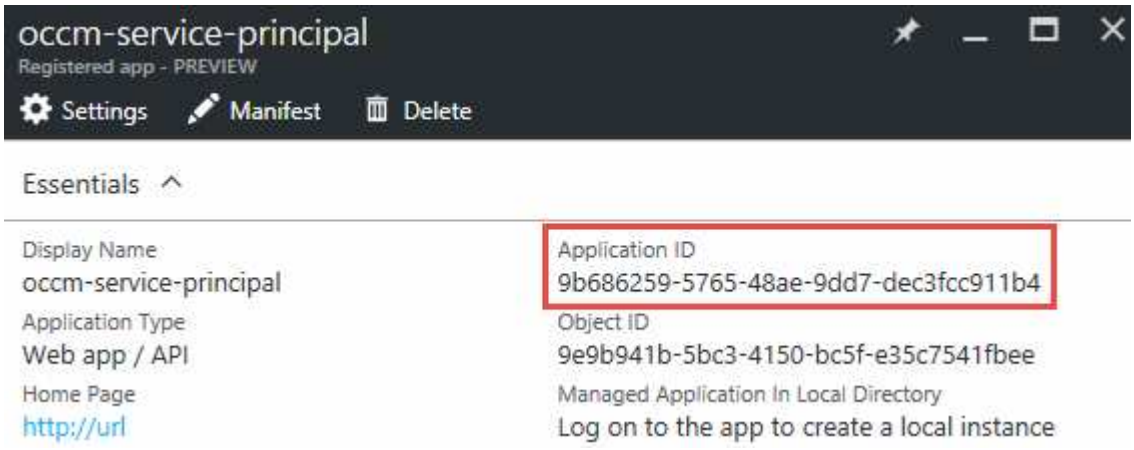
   b. Introduzca una descripción, seleccione una duración y, a continuación, haga clic en **Guardar**.

   c. Copie el valor clave.

   Necesita introducir el valor de clave al añadir una cuenta de proveedor de cloud a Cloud Manager.

d. Haga clic en **Propiedades** y, a continuación, copie el ID de la aplicación para el principal de servicio.

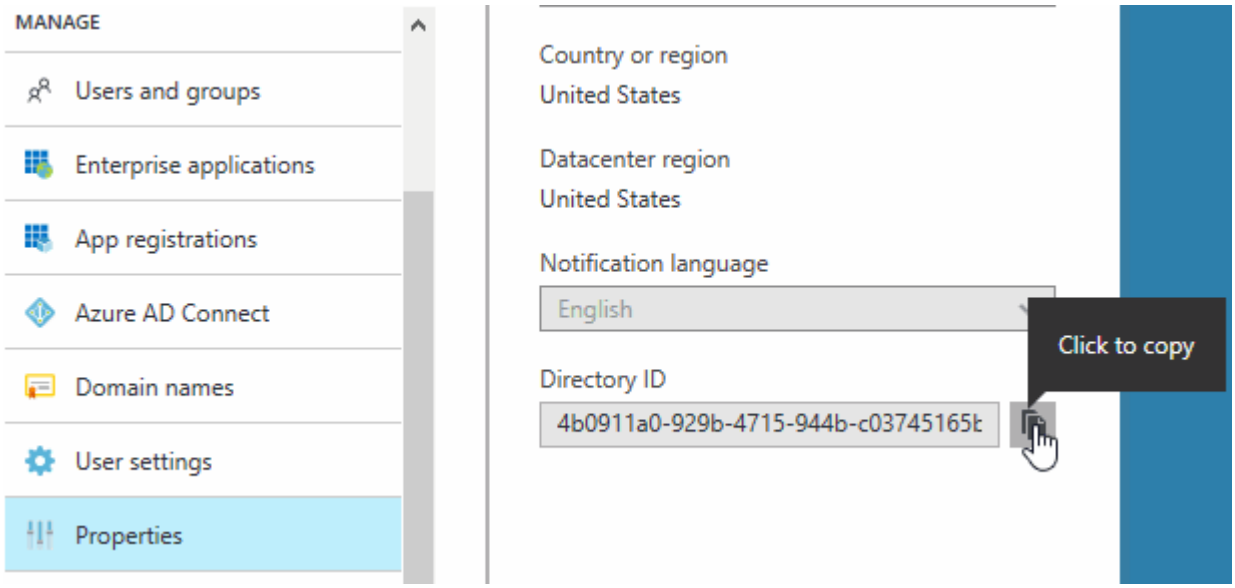
   Al igual que el valor de la clave, debe introducir el ID de aplicación en Cloud Manager cuando añada una cuenta de proveedor de cloud a Cloud Manager.



6. Obtenga el ID de inquilino de Active Directory para su organización:

   a. En el menú Active Directory, haga clic en **Propiedades**.

   b. Copie el ID del directorio.



   Al igual que el ID de aplicación y la clave de aplicación, debe introducir el ID de inquilino de Active Directory al agregar una cuenta de proveedor de cloud a Cloud Manager.

Resultado

Ahora debería tener un principal de servicio de Active Directory y debería haber copiado el ID de aplicación, la clave de aplicación y el ID de inquilino de Active Directory. Debe introducir esta información en Cloud Manager cuando añada una cuenta de proveedor de cloud.

Asignación del rol de operador de Cloud Manager al director de servicio

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

Acerca de esta tarea

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.

Pasos

1. En el portal de Azure, seleccione **Suscripciones** en el panel izquierdo.
2. Seleccione la suscripción.
3. Haga clic en **Control de acceso (IAM)** y a continuación, haga clic en **Agregar**.
4. Seleccione el rol **operador de Cloud Manager de OnCommand**.
5. Busque el nombre de la aplicación (no puede encontrarlo en la lista desplazándose).
6. Seleccione la aplicación, haga clic en **Seleccionar** y, a continuación, haga clic en **Aceptar**.

Resultado

El principal de servicio para Cloud Manager ahora tiene los permisos de Azure necesarios.

Adición de cuentas de Azure a Cloud Manager

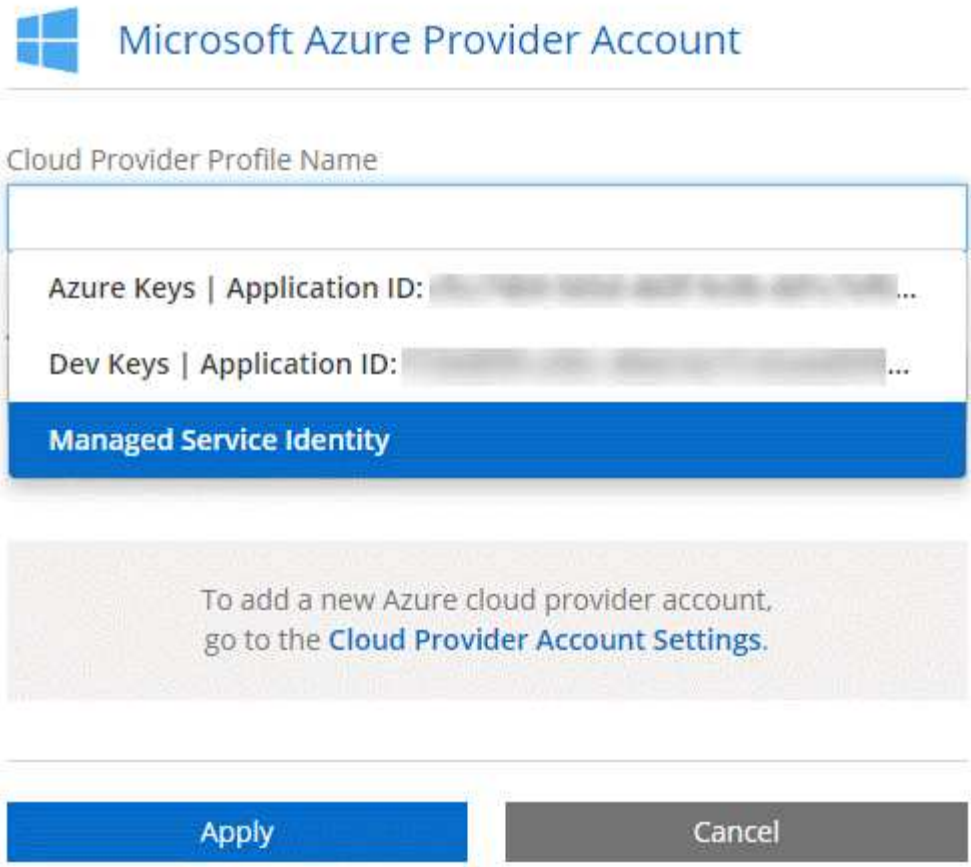
Después de proporcionar una cuenta de Azure con los permisos necesarios, puede añadir la cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en la lista desplegable de tareas y, a continuación, seleccione **Configuración de cuenta**.
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.
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 inicial "cuenta del proveedor de cloud" 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.

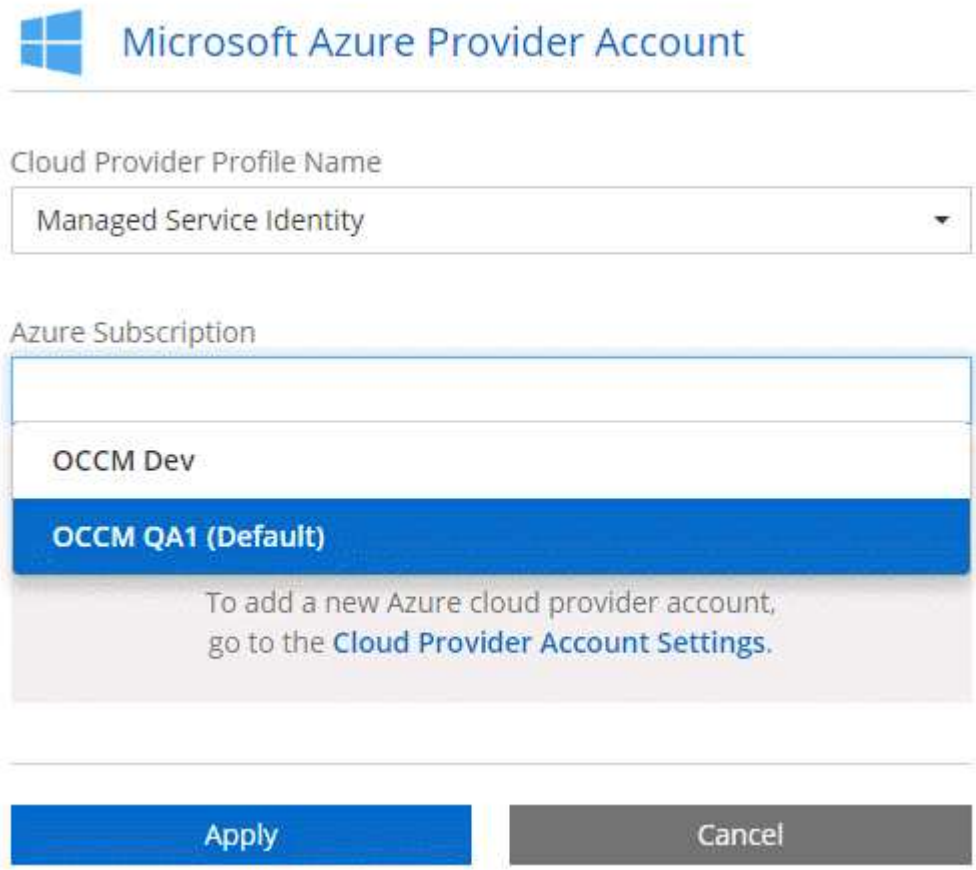
      - Asigne acceso a una **máquina virtual**.

- 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.



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 parte superior derecha de la consola de Cloud Manager, haga clic en la lista desplegable de tareas y,

a continuación, seleccione **Configuración de cuenta**.

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

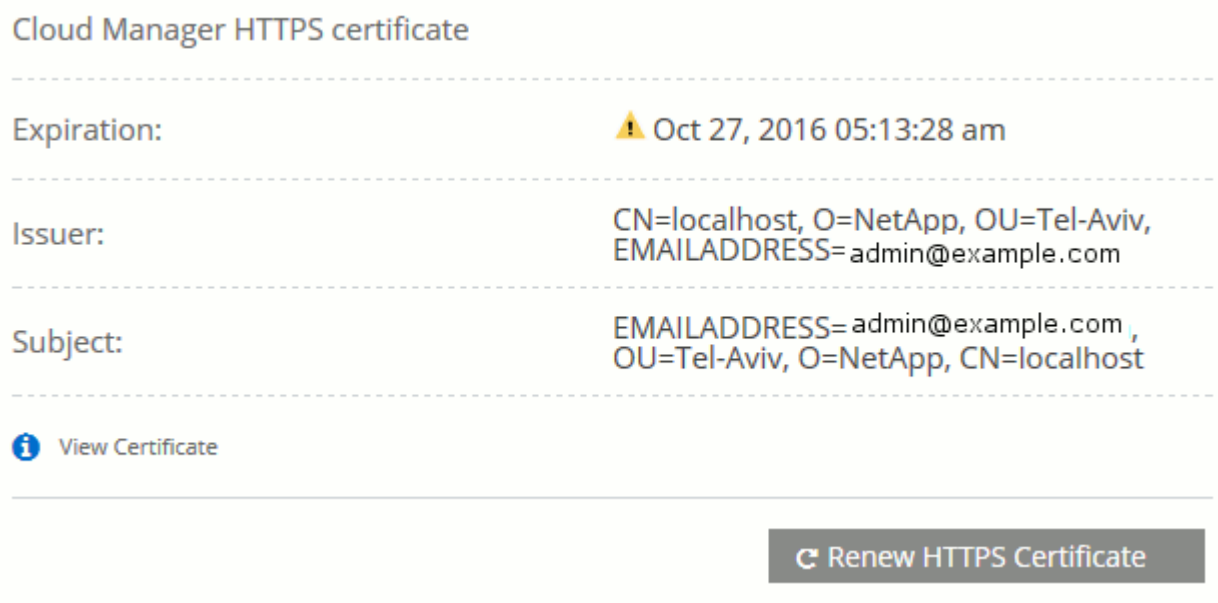
1. En la parte superior derecha de la consola de Cloud Manager, haga clic en la lista desplegable de tareas y, a continuación, seleccione **Configuración HTTPS**.
2. En la página HTTPS Setup, instale un certificado generando una solicitud de firma de certificación (CSR) o instalando su propio certificado 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**.

Opción	Descripción
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:



Configurar usuarios e inquilinos

Cloud Manager le permite añadir usuarios de Cloud Central adicionales a Cloud Manager y aislar entornos de trabajo mediante el uso de inquilinos.

Añadiendo usuarios a Cloud Manager

Si otros usuarios necesitan usar su sistema Cloud Manager, deben registrarse para obtener una cuenta en Cloud Central de NetApp. A continuación, puede agregar usuarios a Cloud Manager.

Pasos

1. Si el usuario aún no tiene una cuenta en Cloud Central de NetApp, envíenos un enlace a su sistema Cloud Manager y haga que se registren.

   Espere hasta que el usuario confirme que se ha registrado para una cuenta.

2. En Cloud Manager, haga clic en el icono de usuario y, a continuación, haga clic en **Ver usuarios**.
3. Haga clic en **Nuevo usuario**.

4. Introduzca la dirección de correo electrónico asociada a la cuenta de usuario, seleccione una función y haga clic en **Agregar**.

El futuro

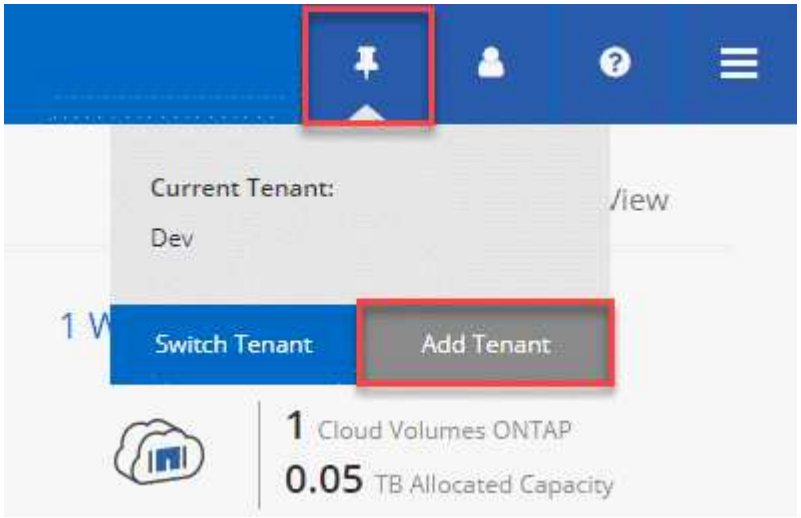
Informe al usuario de que ahora puede iniciar sesión en el sistema Cloud Manager.

Creación de inquilinos

Los inquilinos le permiten aislar sus entornos de trabajo en grupos separados. Se crean uno o más entornos de trabajo dentro de un inquilino. "Más información acerca de los inquilinos".

Pasos

1. Haga clic en el icono arrendatarios y, a continuación, haga clic en **Agregar arrendatario**.



2. Introduzca un nombre, una descripción y un centro de costes, si es necesario.
3. Haga clic en **Guardar**.

El futuro

Ahora puede cambiar a este nuevo inquilino y agregar administradores de inquilino y administradores de entorno de trabajo a este inquilino.

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.

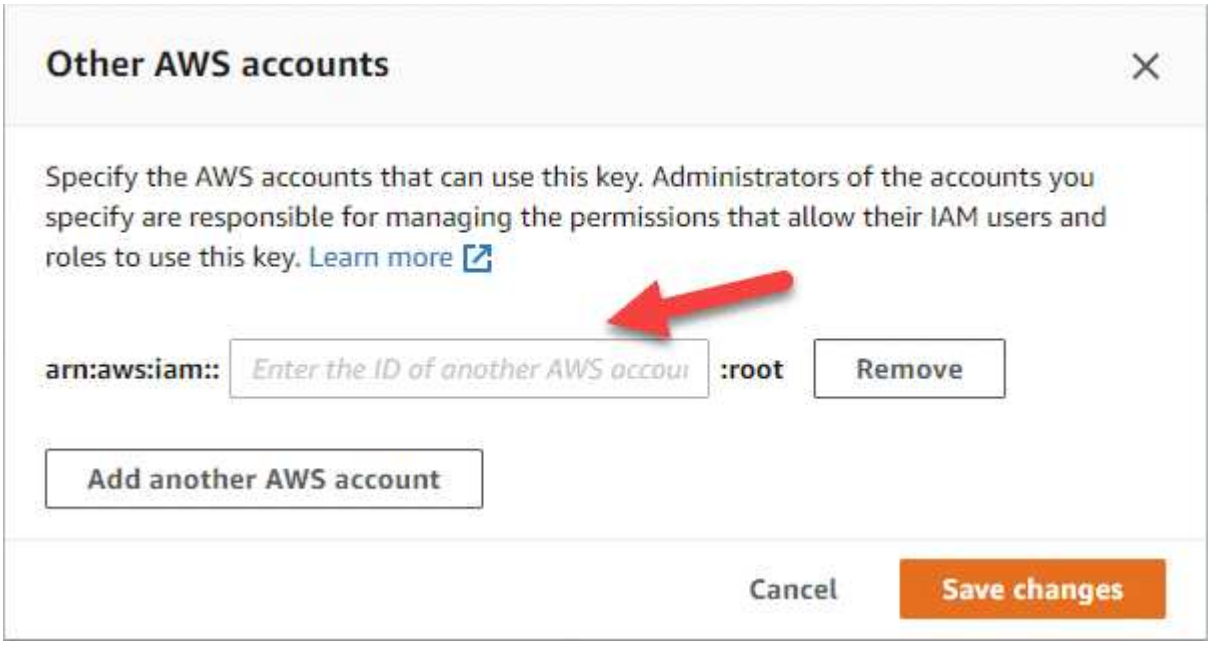
   b. Seleccione la tecla.

   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

Debe configurar la red para que Cloud Manager pueda poner en marcha sistemas de Cloud Volumes ONTAP en AWS o en Microsoft Azure. 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 de AWS y VNets de Azure en los que desee poner en marcha Cloud Volumes ONTAP.

Por ejemplo, si instala Cloud Manager en su red corporativa, debe configurar una conexión VPN con el VPC de AWS o vnet de Azure 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.

Acceso saliente a Internet 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://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 registro de soporte y licencia.
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.

Acceso saliente a Internet 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.

Puntos finales	Específico
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://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 registro de soporte y licencia.
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.

Acceso saliente a Internet 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.

Acceso saliente a Internet 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"
- 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.

> ¿Busca la lista de extremos a los que Cloud Manager requiere acceso? Ahora se mantienen en una única ubicación. "Haga clic aquí para obtener más información".

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)".

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: Implementación de la referencia de inicio rápido de Active Directory Domain Services en AWS Cloud".

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".

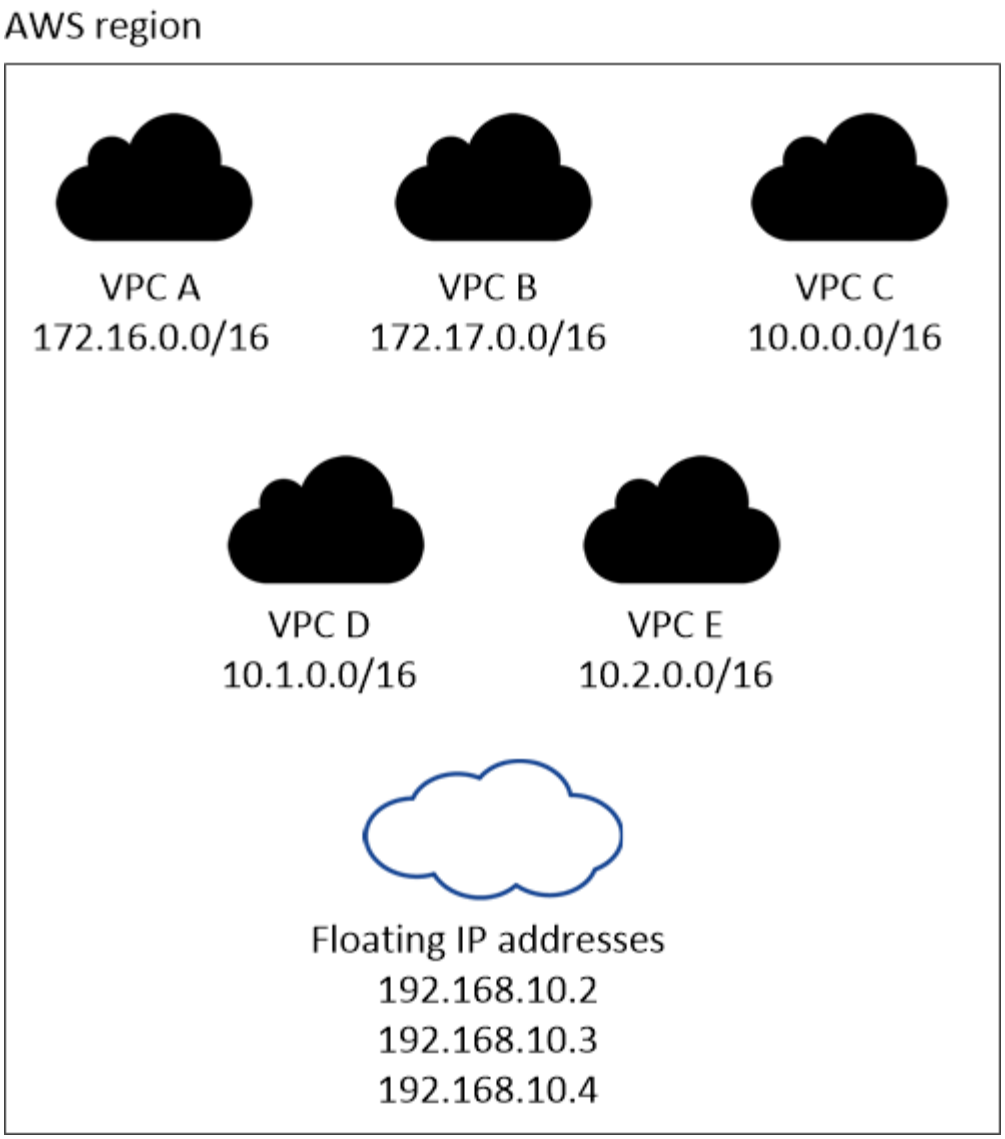
Una dirección IP flotante es para la gestión del clúster, otra para los datos NFS/CIFS del nodo 1 y otra para los datos NFS/CIFS del nodo 2. Una cuarta dirección IP flotante para la gestión de SVM es opcional.

> 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".

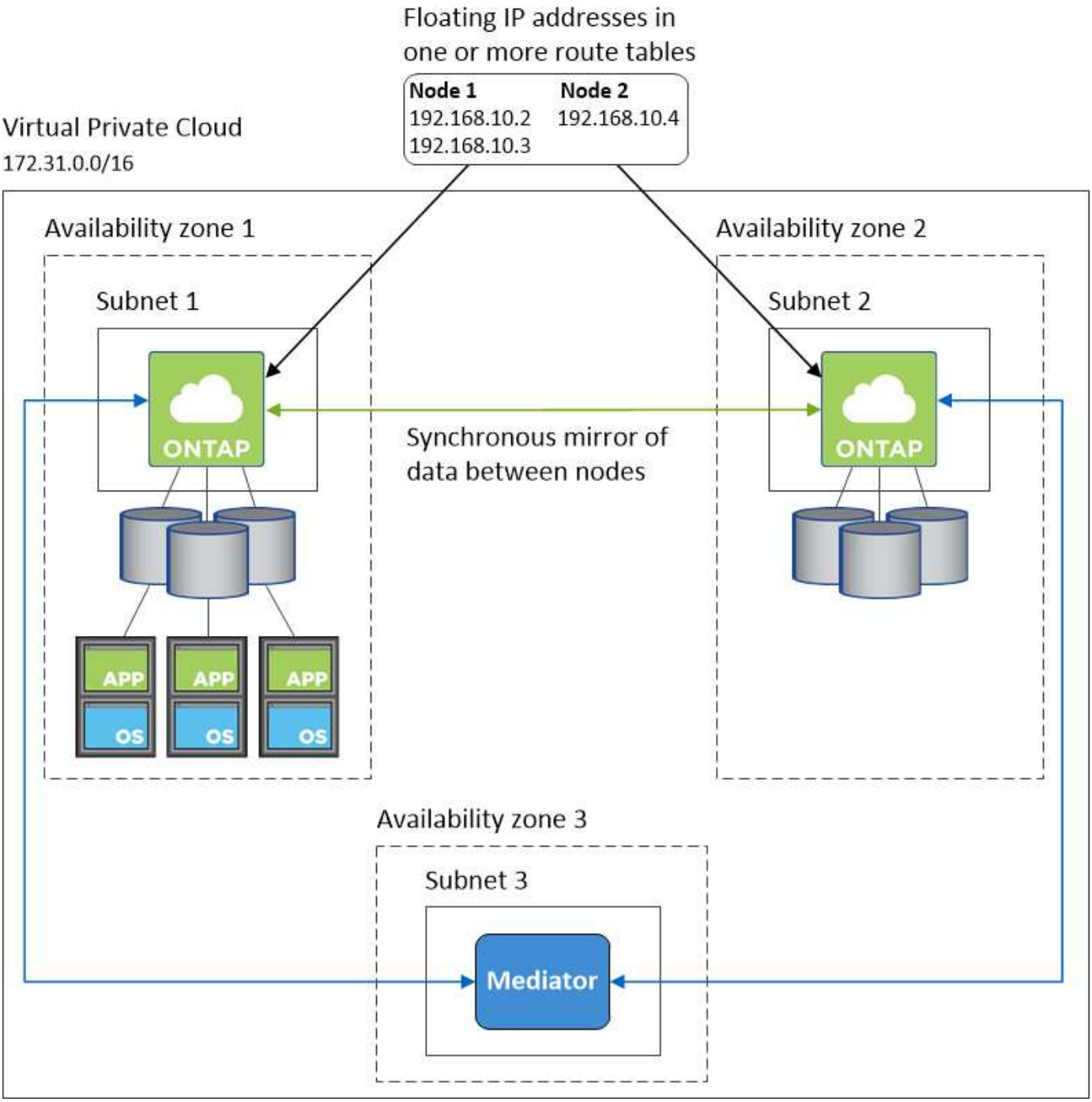
Conexión a herramientas de gestión de NetApp

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

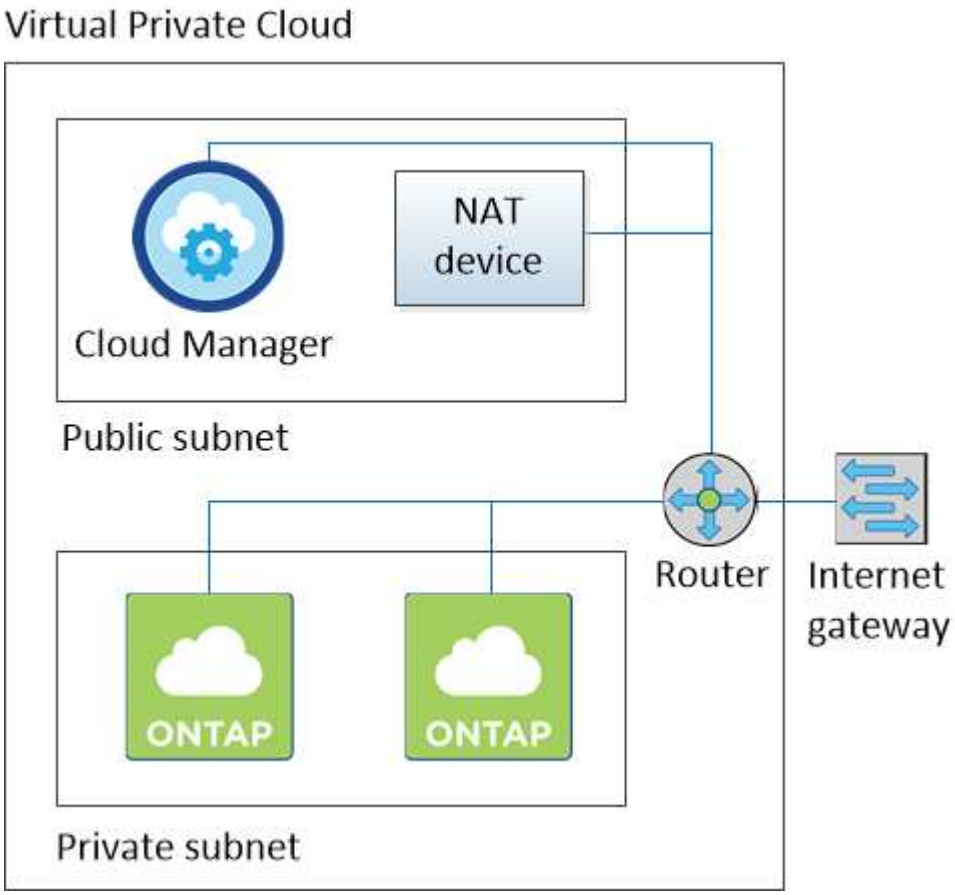
Esta configuración de VPC incluye subredes públicas y privadas, una puerta de enlace de Internet que conecta el VPC a Internet y una instancia de NAT o de NAT en la subred pública que permita el tráfico de

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

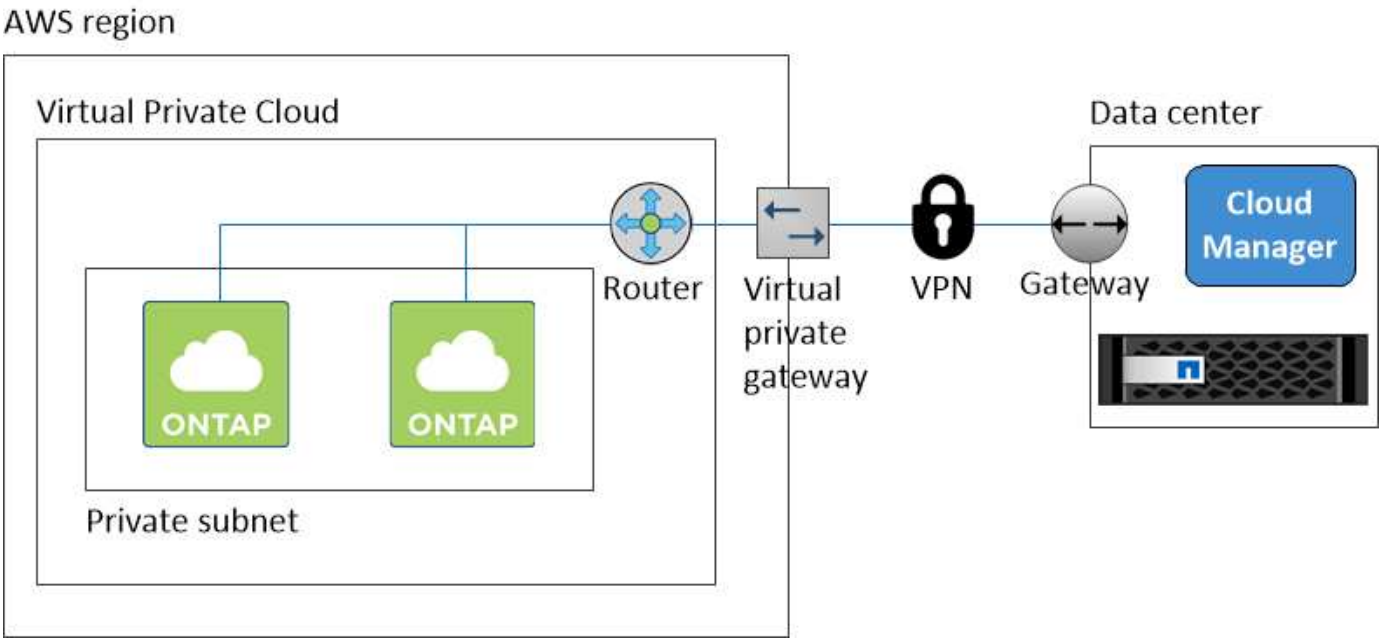
Esta configuración de VPC es una configuración de cloud híbrido en la que Cloud Volumes ONTAP se convierte en una extensión del entorno privado. La configuración incluye una subred privada y una puerta de enlace privada virtual con una conexión VPN a la red. El enrutamiento a través del túnel VPN permite 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

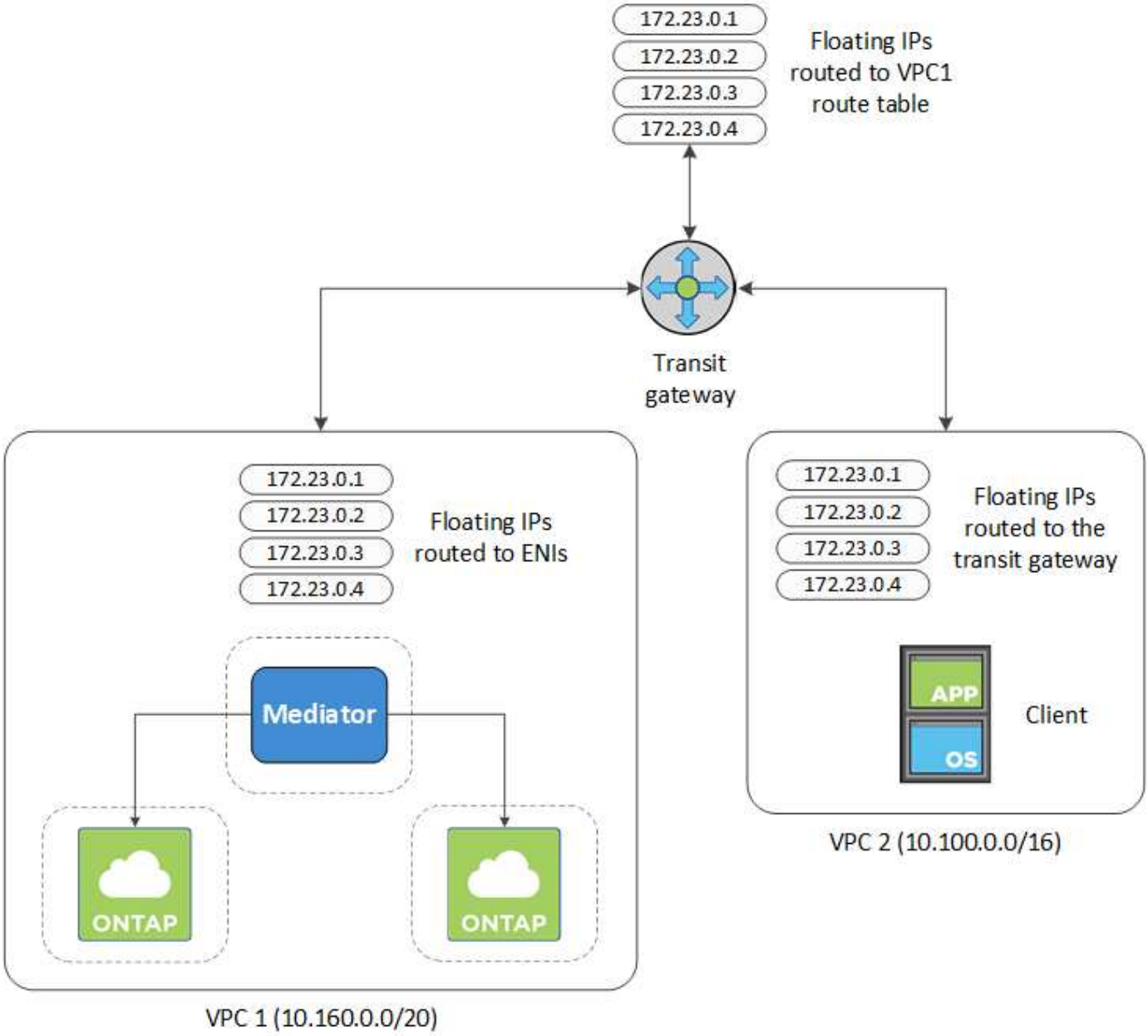
Configure una puerta de enlace de tránsito de AWS para permitir el acceso a las direcciones IP flotantes de un par de alta disponibilidad desde fuera del VPC donde reside el par de alta disponibilidad.

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:

NFS & CIFS access from within the VPC using Floating IP

Auto failover

Cluster Management :	172.23.0.1
Data (nfs,cifs) :	**Node 1:** 172.23.0.2 | **Node 2:** 172.23.0.3

Access

SVM Management :	172.23.0.4

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.

Transit Gateway Route Table: tgw-rtb-0ea8ee291c7aeddd3

Details | Associations | Propagations | **Routes** | Tags

The table below will return a maximum of 1000 routes. Narrow the filter or use export routes to view more routes.

Create route | Replace route | Delete route

Filter by attributes or search by keyword

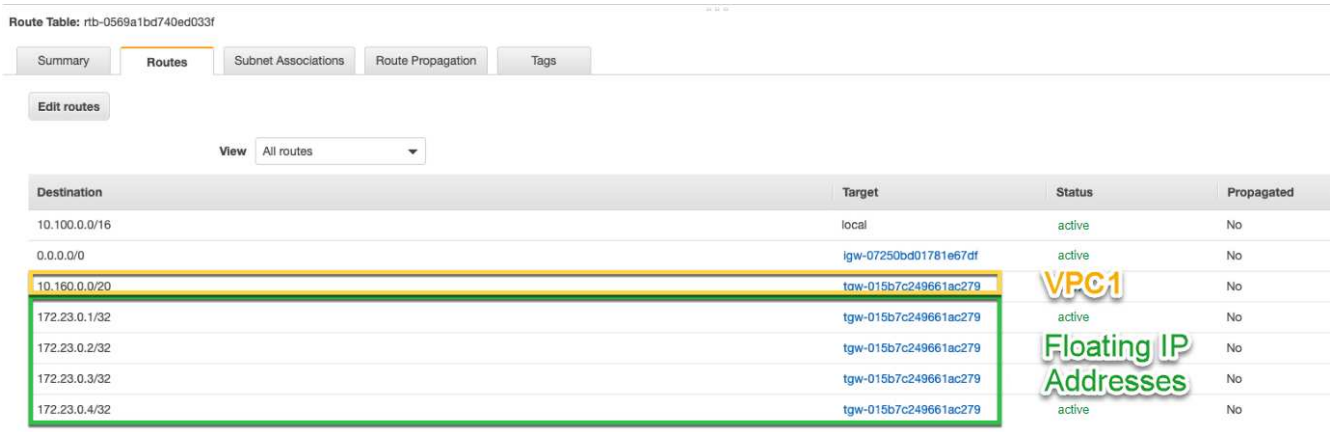
CIDR	Attachment	Resource type	Route type	Route state
10.100.0.0/16	tgw-attach-05e77bd34e2ff91f8 | vpc-0b2bc30e0dc8e0db1	VPC2	propagated	active
10.160.0.0/20	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC1	propagated	active
172.23.0.1/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC	static	active
172.23.0.2/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	VPC	static	active
172.23.0.3/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603	Floating IP Addresses	static	active
172.23.0.4/32	tgw-attach-00eba3eac3250d7db | vpc-673ae603		static	active

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.

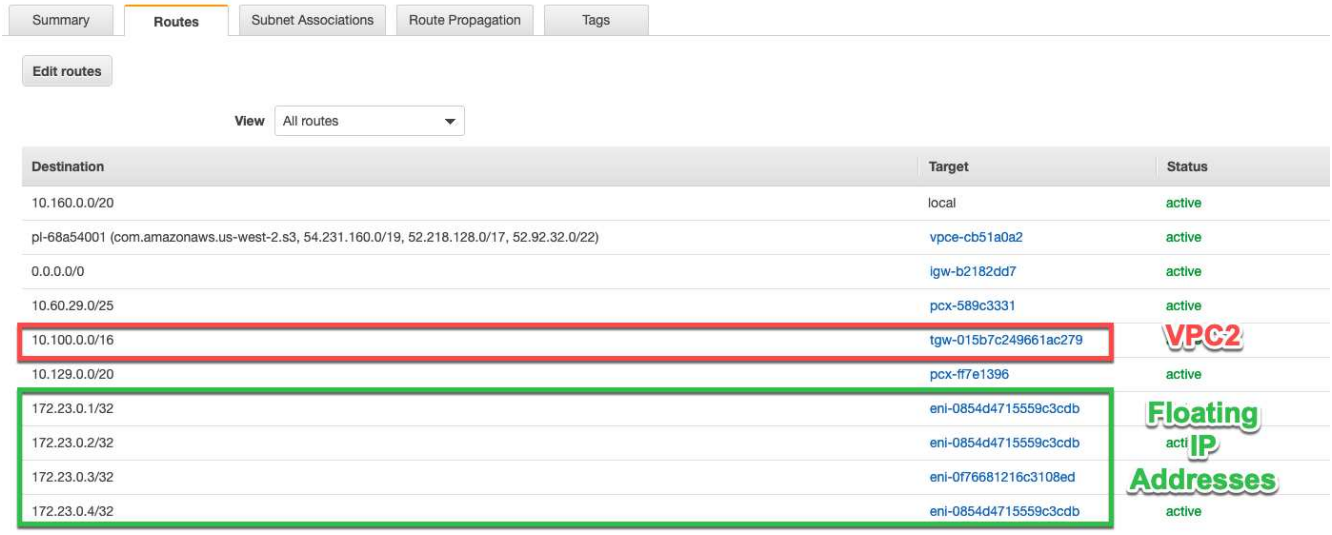
      La siguiente imagen de ejemplo muestra la tabla de rutas para VPC 2, que incluye las rutas hasta VPC 1 y las direcciones IP flotantes.



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.

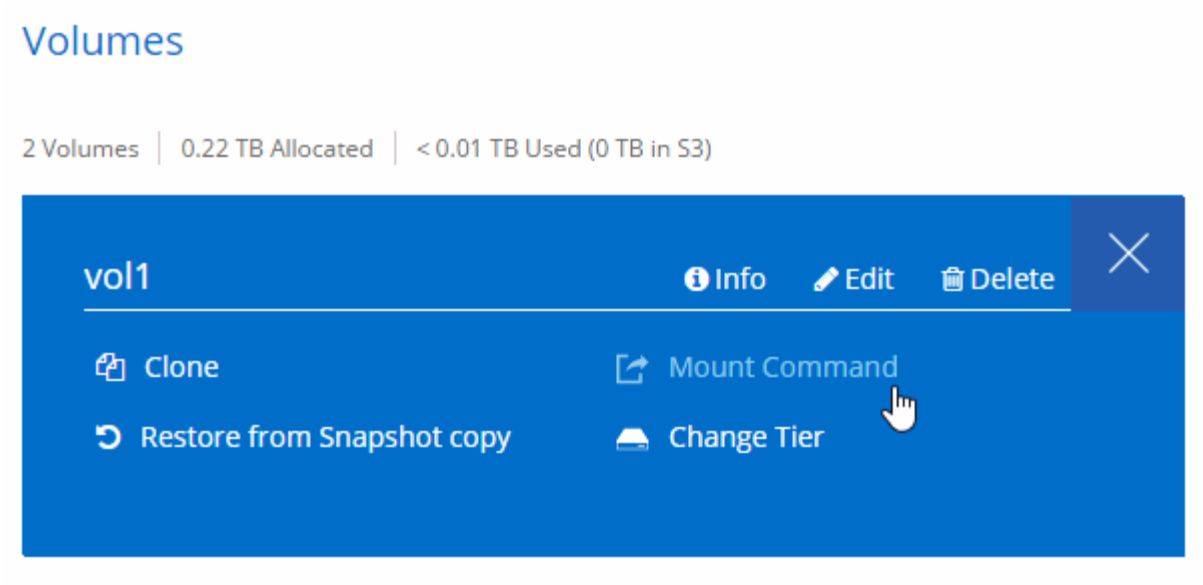
   Este paso es importante porque completa el enrutamiento entre las VPC.

   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

Debe configurar las redes de Azure para que los sistemas Cloud Volumes ONTAP funcionen correctamente.

> ¿Busca la lista de extremos a los que Cloud Manager requiere acceso? Ahora se mantienen en una única ubicación. "Haga clic aquí para obtener más información".

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 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

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 Azure Blob Storage para organización en niveles de los datos

Si desea organizar en niveles datos inactivos en almacenamiento de Azure Blob, no tiene que configurar un extremo de servicio vnet siempre que Cloud Manager tenga los permisos necesarios:

```
"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".

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.

Tipos de instancia de AWS EC2 admitidos

t3.medium (recomendado), t2.medium y m4.large

Tamaños de máquina virtual de Azure admitidos

A2, D2 v2 o D2 v3 (según disponibilidad)

Sistemas operativos compatibles

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

  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.

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 para AWS"
   - "Requisitos de red para Cloud Volumes ONTAP para Azure"
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-V3.6.3.sh
   . Ejecute el script de instalación:
   ```

   ```
   ./OnCommandCloudManager-V3.6.3.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 para obtener una cuenta de Cloud Central de NetApp o inicie sesión si ya dispone de una.
8. Al registrarse o iniciar sesión, Cloud Manager agrega automáticamente su cuenta de usuario como administrador para este sistema.
9. Después de iniciar sesión, escriba un nombre para este sistema Cloud Manager.

Después de terminar

Configure permisos para sus cuentas de AWS y Azure para que Cloud Manager pueda poner en marcha Cloud Volumes ONTAP:

- Si desea implementar Cloud Volumes ONTAP en AWS, "Configure una cuenta de AWS y, a continuación, añádala a Cloud Manager".
- Si desea implementar Cloud Volumes ONTAP en Azure, "Configure una cuenta de Azure y, a continuación, añádala a Cloud Manager".

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 con la opción 1-Click.

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:

      "OnCommand Cloud Manager de NetApp: Políticas de AWS y Azure"

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. Vaya a la "Cloud Manager en el mercado de AWS".
3. Haga clic en **continuar**.
4. En la ficha Inicio personalizado, haga clic en **Iniciar con la consola EC2** para su región y, a continuación, realice las selecciones siguientes:

   a. En función de la disponibilidad de la región, elija el tipo de instancia t3.medium (recomendado), t2.medium o m4.Large.

   b. Seleccione un VPC, una subred, un rol de IAM y otras opciones de configuración que se adapten a sus requisitos.

   c. Mantenga las opciones de almacenamiento predeterminadas.

   d. Introduzca etiquetas para la instancia, si lo desea.

   e. Especifique los métodos de conexión necesarios para la instancia de Cloud Manager: SSH, HTTP y HTTPS.

   f. Haga clic en **Iniciar**.

Resultado

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

Después de terminar

Inicie sesión en Cloud Manager introduciendo la dirección IP pública o la dirección IP privada en un navegador web y, a continuación, complete el asistente de configuración.

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

   Al iniciar sesión, Cloud Manager agrega automáticamente su cuenta de usuario como administrador para este sistema.

6. Después de iniciar sesión, escriba un nombre para el sistema Cloud Manager.

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_3.6.1.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. Busque Cloud Manager de OnCommand en el portal gubernamental de Azure Estados Unidos.
2. 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.

3. 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.

4. 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

   Al iniciar sesión, Cloud Manager agrega automáticamente su cuenta de usuario como administrador para este sistema.

5. Después de iniciar sesión, escriba un nombre para el sistema Cloud Manager.

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_3.6.1.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.