Administre Cloud Manager

Cloud Manager 3.8

NetApp
March 25, 2024

Tabla de contenidos

Administre Cloud Manager

Buscar el ID del sistema de Cloud Manager

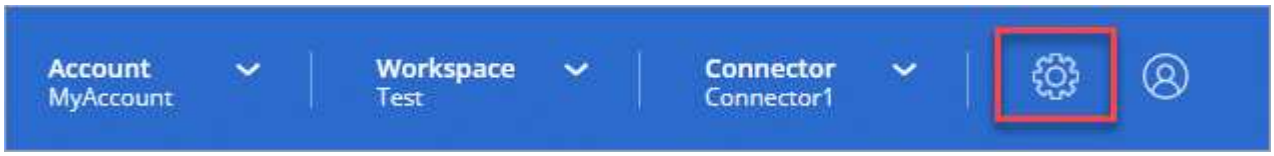
Para ayudarle a comenzar, su representante de NetApp puede pedirle el ID de sistema de Cloud Manager. El ID se utiliza normalmente para licencias y solución de problemas.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

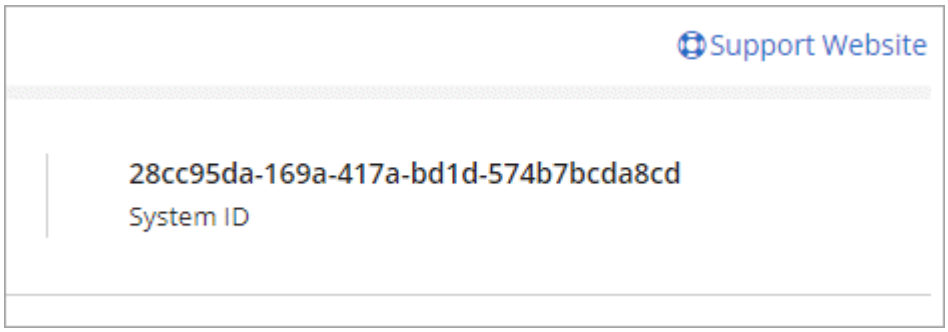
1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración.



2. Haga clic en **Panel de soporte**.

   El ID del sistema aparece en la parte superior derecha.

   ejemplo



Gestionar conectores

Gestión de conectores existentes

Después de crear uno o más conectores, puede gestionarlos cambiando entre conectores, conectándose a la interfaz de usuario local que se ejecuta en un conector, entre otros.

Cambio entre conectores

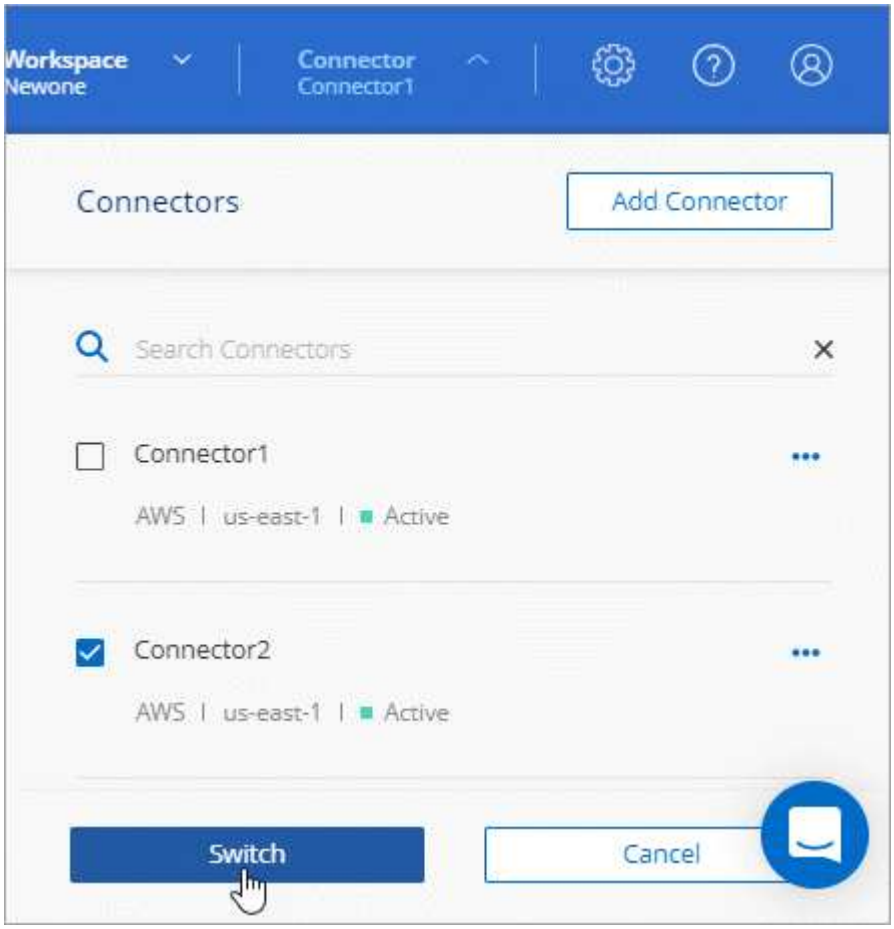
Si tiene varios conectores, puede alternar entre ellos para ver los entornos de trabajo asociados a un conector específico.

Por ejemplo, digamos que trabaja en un entorno multicloud. Es posible que tenga un conector en AWS y otro en Google Cloud. Tendría que cambiar entre estos conectores para gestionar los sistemas Cloud Volumes

ONTAP que se ejecutan en esas nubes.

Paso

1. Haga clic en el menú desplegable **conector**, seleccione otro conector y, a continuación, haga clic en **conmutador**.



Cloud Manager actualiza y muestra los entornos de trabajo asociados con el conector seleccionado.

Obtener acceso a la interfaz de usuario local

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. Esta interfaz es necesaria para algunas tareas que se deben realizar desde el propio conector:

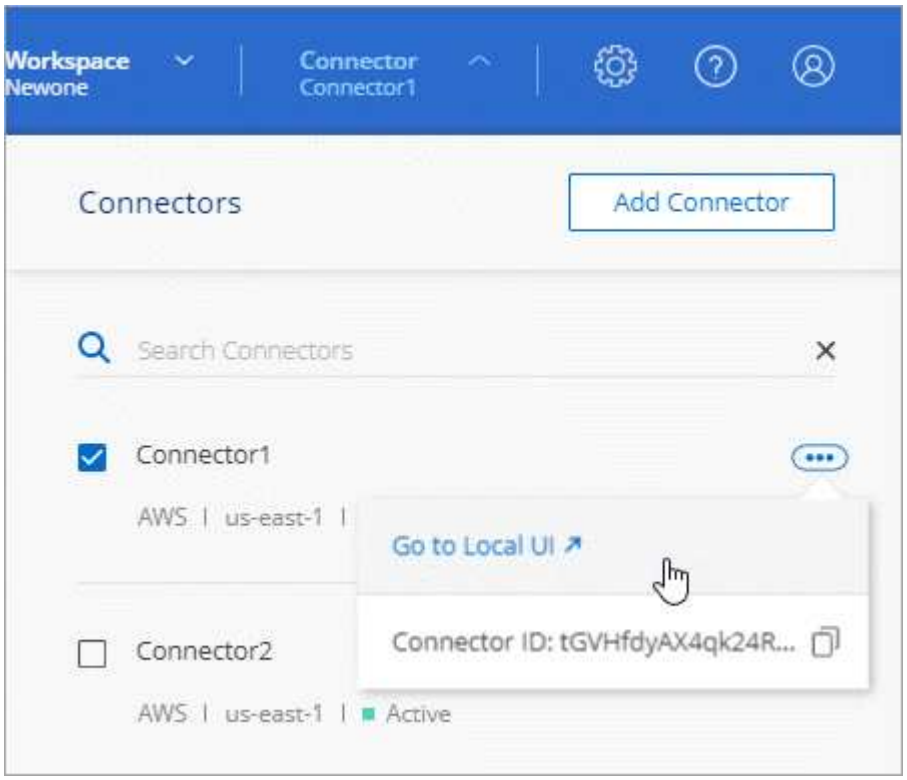
- "Establecimiento de un servidor proxy"
- Instalación de un parche (Normalmente, trabajará con el personal de NetApp para instalar un parche).
- Descargando mensajes de AutoSupport (Normalmente dirigido por el personal de NetApp cuando tiene problemas)

Pasos

1. "Inicie sesión en la interfaz del SaaS de Cloud Manager" Desde un equipo que tiene una conexión de red a la instancia de conector.

   Si el conector no tiene una dirección IP pública, necesitará una conexión VPN o deberá conectarse desde un host de salto que esté en la misma red que el conector.

2. Haga clic en el menú desplegable **conector**, haga clic en el menú de acción de un conector y, a continuación, haga clic en **Ir a interfaz de usuario local**.



La interfaz de Cloud Manager que se ejecuta en el conector se carga en una nueva pestaña del navegador.

Quitando conectores de Cloud Manager

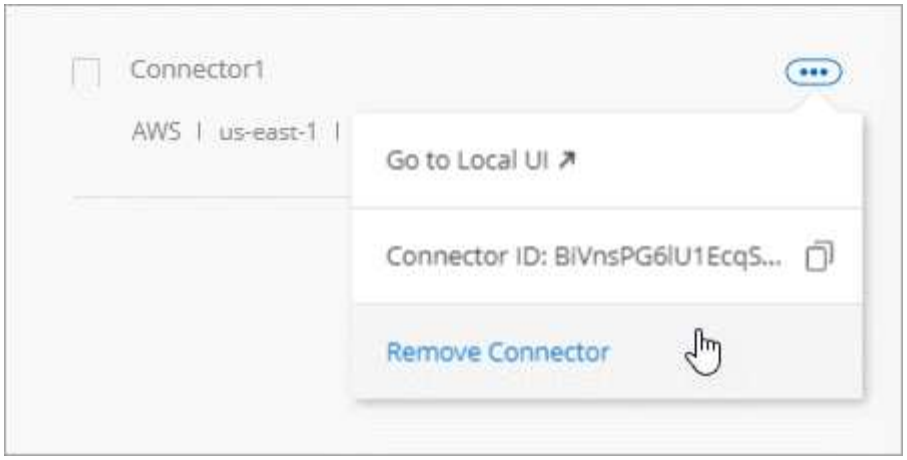
Si un conector está inactivo, puede quitarlo de la lista de conectores de Cloud Manager. Puede hacerlo si ha eliminado la máquina virtual conector o si ha desinstalado el software conector.

Tenga en cuenta lo siguiente sobre la extracción de un conector:

- Esta acción no elimina la máquina virtual.
- No se puede revertir esta acción. Una vez que se quita un conector de Cloud Manager, no se puede volver a añadir a Cloud Manager.

Pasos

1. Haga clic en el menú desplegable conector del encabezado Cloud Manager.
2. Haga clic en el menú de acción de un conector inactivo y haga clic en **Quitar conector**.



3. Introduzca el nombre del conector que desea confirmar y, a continuación, haga clic en Quitar.

Resultado

Cloud Manager quita el conector de sus registros.

Desinstalación del software del conector

El conector incluye una secuencia de comandos de desinstalación que puede utilizar para desinstalar el software para solucionar problemas o para quitar permanentemente el software del host.

Paso

1. Desde el host Linux, ejecute el script de desinstalación:

   /opt/application/netapp/cloudmanager/bin/uninstall.sh [silent]

   silent ejecuta la secuencia de comandos sin que se le solicite confirmación.

¿y las actualizaciones de software?

El conector actualiza automáticamente su software a la última versión, siempre que lo haya hecho "acceso a internet de salida" para obtener la actualización de software.

Más formas de crear conectores

Requisitos del host del conector

El software del conector debe ejecutarse en un host que cumpla con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de puerto, etc.

Se requiere un host dedicado

El conector no es compatible con un host compartido con otras aplicaciones. El host debe ser un host dedicado.

CPU

4 núcleos o 4 vCPU

RAM

14 GB

Tipo de instancia de AWS EC2

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos t3.xlarge y el uso de ese tipo de instancia al implementar el conector directamente desde Cloud Manager.

Tamaño de la máquina virtual de Azure

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos DS3 v2 y utilizar ese tamaño de equipo virtual al implementar el conector directamente desde Cloud Manager.

Tipo de máquina GCP

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Le recomendamos n1-standard-4 y utilizar ese tipo de máquina cuando ponga en marcha el conector directamente desde Cloud Manager.

Sistemas operativos compatibles

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  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 necesario de terceros durante la instalación del conector.

  El conector 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?"^]

Espacio en disco en /opt

Debe haber 100 GB de espacio disponibles

Acceso a Internet de salida

Se requiere acceso saliente a Internet para instalar el conector y el conector para gestionar recursos y procesos dentro de su entorno de cloud público. Para ver una lista de extremos, consulte "Requisitos de red para el conector".

Creación de un conector desde AWS Marketplace

Es mejor crear un conector directamente desde Cloud Manager, pero puede iniciar un conector desde AWS Marketplace, si prefiere no especificar claves de acceso de AWS. Después de crear y configurar el conector, Cloud Manager lo utilizará automáticamente al crear nuevos entornos de trabajo.

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"

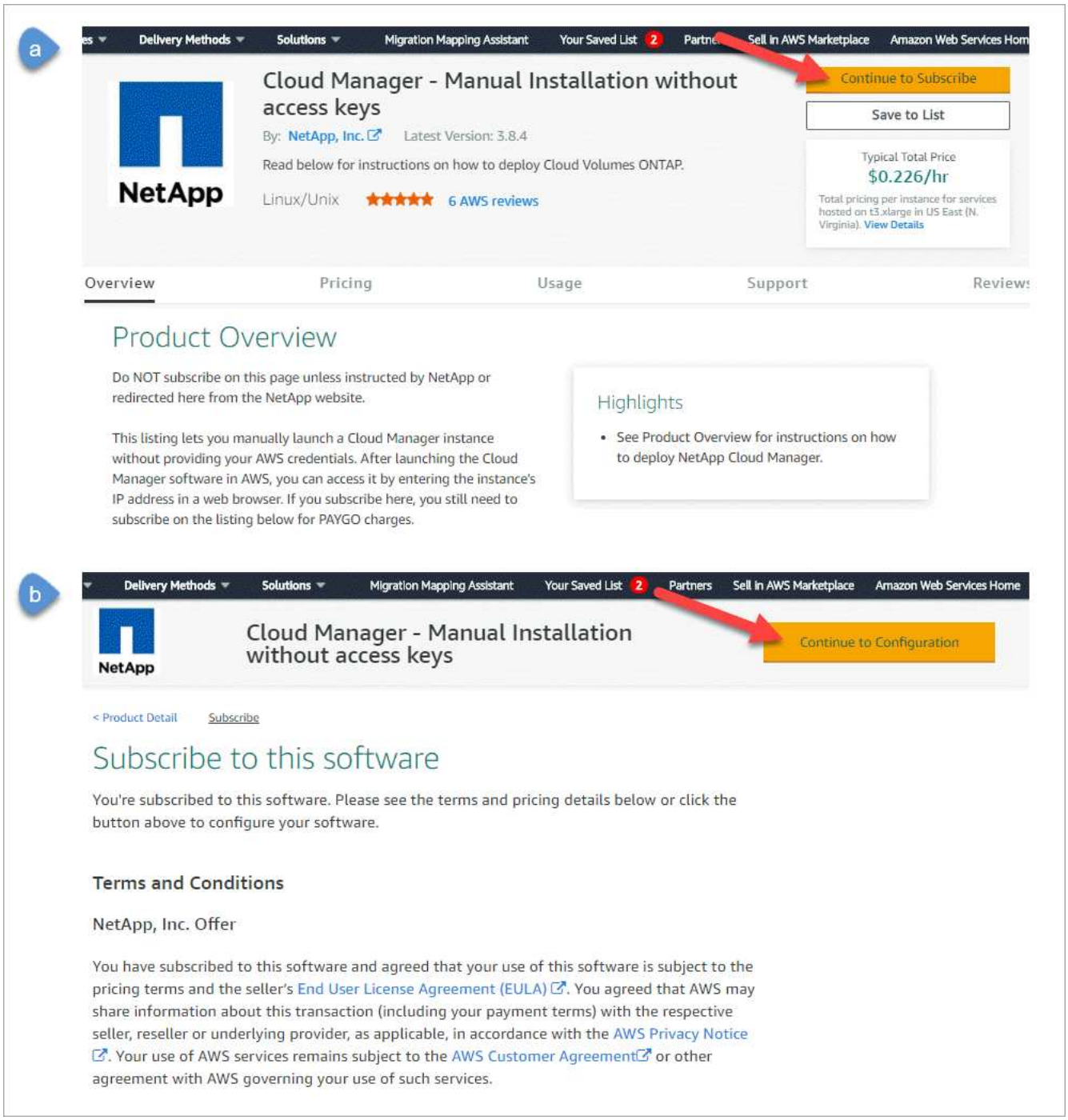
b. Desde la consola de IAM, cree su propia política copiando y pegando el texto de la política IAM de Cloud Manager.

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. Ahora vaya a la "Cloud Manager en el mercado de AWS" Para poner en marcha Cloud Manager desde una AMI.

   El usuario de IAM debe disponer de permisos de AWS Marketplace para suscribirse y cancelar la suscripción.

3. En la página Marketplace, haga clic en **continuar a Suscribirse** y luego haga clic en **continuar a Configuración**.



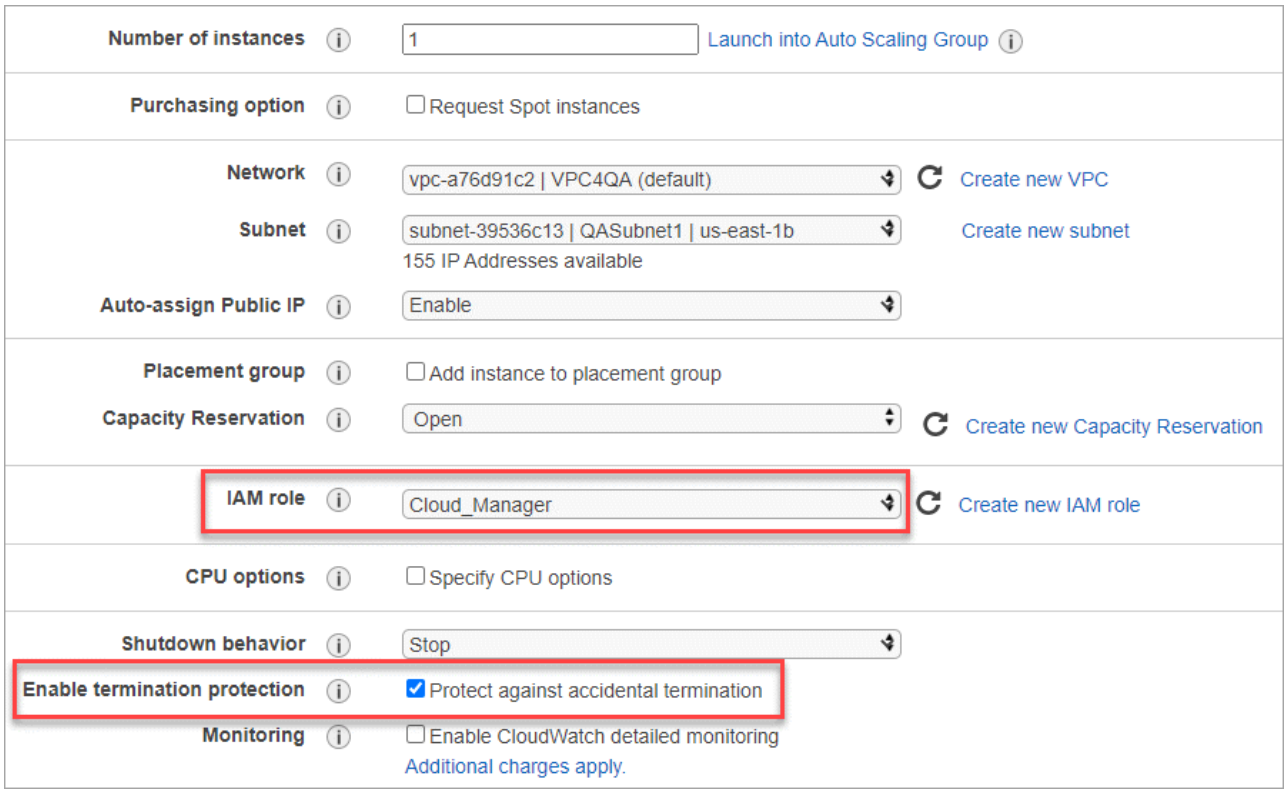
4. Cambie cualquiera de las opciones predeterminadas y haga clic en **continuar a Iniciar**.
5. En **elegir acción**, seleccione **Iniciar a través de EC2** y, a continuación, haga clic en **Iniciar**.

   Estos pasos describen cómo iniciar la instancia desde la consola 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**.

6. 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.xlarge).

     "Revise los requisitos de la instancia".

- **Configurar instancia**: Seleccione un VPC y una subred, elija la función de IAM que creó en el paso 1, habilite la protección de terminación (recomendado) y elija cualquier otra opción de configuración que cumpla 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 conector: 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 del conector deben estar funcionando en aproximadamente cinco minutos.

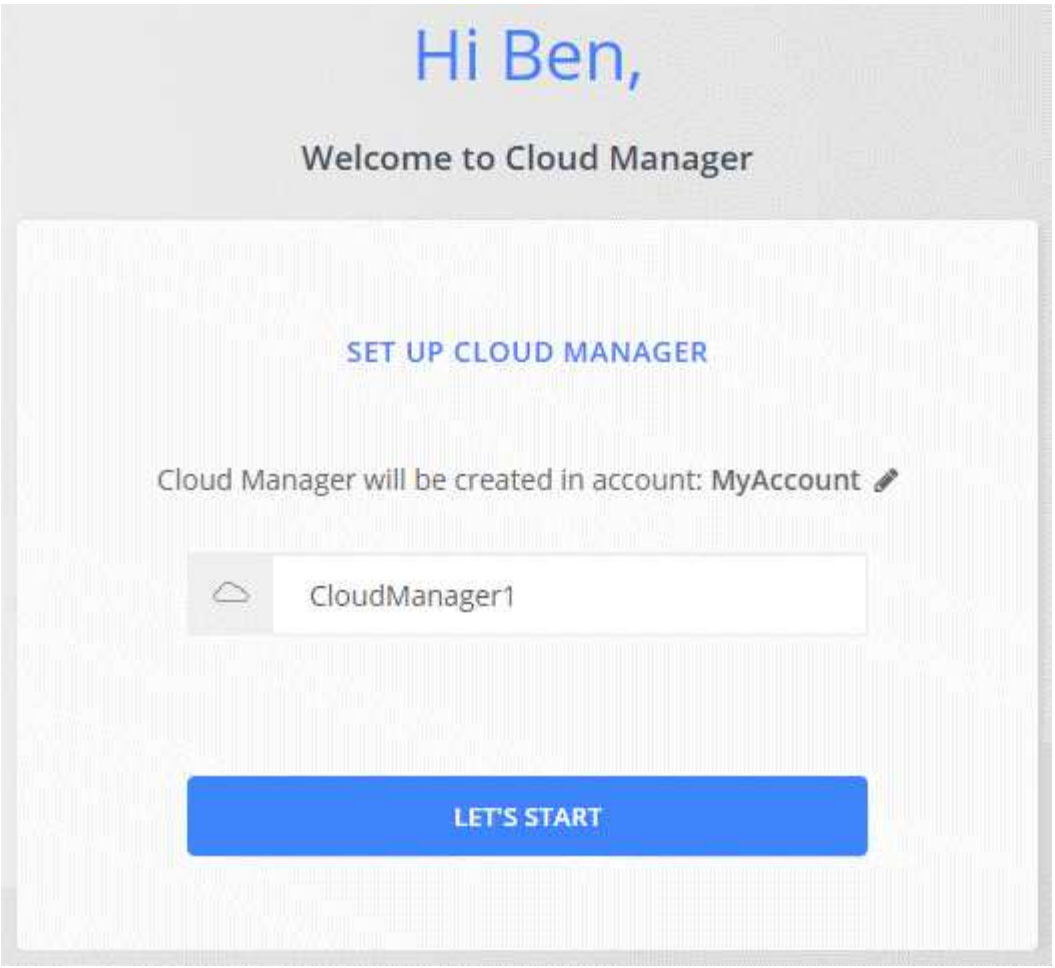
7. Abra un explorador Web desde un host que tenga una conexión con la instancia de Connector e introduzca la siguiente URL:

   http://ipaddress:80

8. Después de iniciar sesión, configure el conector:
   a. Especifique la cuenta de Cloud Central que desea asociar con el conector.

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

   b. Escriba un nombre para el sistema.



Resultado

El conector ya está instalado y configurado con su cuenta de Cloud Central. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará "alterne entre ellos".

Creación de un conector desde Azure Marketplace

Es mejor crear un conector directamente desde Cloud Manager, pero si lo prefiere, puede iniciar un conector desde Azure Marketplace. Después de crear y configurar el conector, Cloud Manager lo utilizará automáticamente al crear nuevos entornos de trabajo.

Creación de un conector en Azure

Implemente el conector en Azure con la imagen en Azure Marketplace y luego inicie sesión en el conector para especificar su cuenta de Cloud Central.

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 un tamaño de máquina virtual que cumpla los requisitos de CPU y RAM. Recomendamos DS3 v2.

  "Revise los requisitos de las máquinas virtuales".

- Para el grupo de seguridad de red, el conector requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

  "Obtenga más información sobre las reglas de grupo de seguridad para el conector".

- En **Gestión**, active **identidad administrada asignada por el sistema** para el conector seleccionando **On**.

  Esta configuración es importante porque una identidad administrada permite que la máquina virtual Connector se identifique a sí misma en Azure Active Directory sin 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. El software de la máquina virtual y el conector debe estar funcionando en aproximadamente cinco minutos.

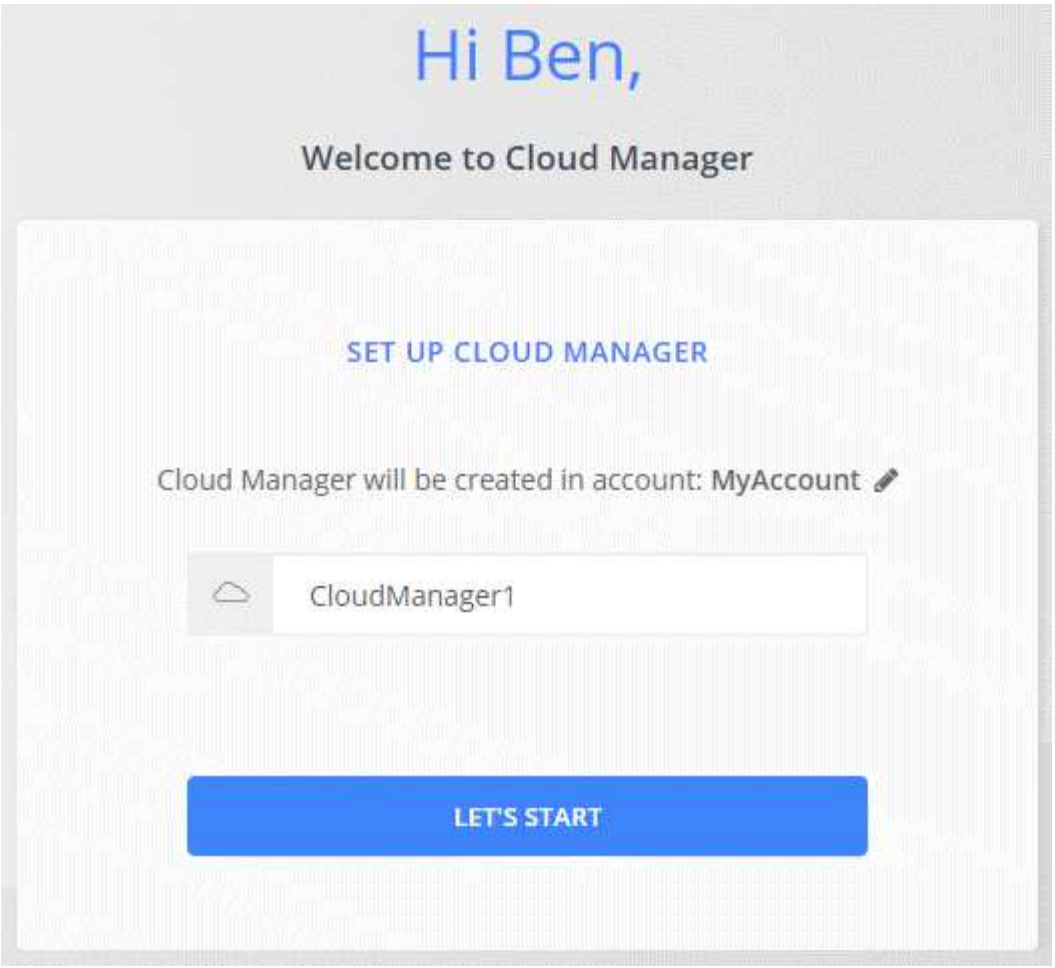
5. Abra un explorador Web desde un host que tenga una conexión con la máquina virtual Connector e introduzca la siguiente URL:

   http://ipaddress:80

6. Después de iniciar sesión, configure el conector:
   a. Especifique la cuenta de Cloud Central que desea asociar con el conector.

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

   b. Escriba un nombre para el sistema.



Resultado

El conector ahora 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

Cuando implementó Connector en Azure, debería haber habilitado un "identidad administrada asignada por el sistema". Ahora debe conceder los permisos de Azure necesarios creando una función personalizada y, a continuación, asignando la función a la máquina virtual Connector 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_3.8.7.json
   ```

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

2. Asigne el rol a la máquina virtual conector 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**.

        Es el nombre predeterminado que se proporciona en la "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 Connector.
      - Seleccione la máquina virtual conector.
      - Haga clic en **Guardar**.
   d. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

Resultado

Connector ahora tiene los permisos que necesita para gestionar recursos y procesos en su entorno de cloud público. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará "alterne entre ellos".

Instalar el software del conector en un host Linux existente

La forma más común de crear un conector es directamente desde Cloud Manager o desde el mercado de un proveedor de cloud. Pero tiene la opción de descargar e instalar el software Connector en un host Linux existente en su red o en la nube.

Si desea crear un sistema Cloud Volumes ONTAP en Google Cloud, también debe tener un conector en Google Cloud. No puede utilizar un conector que se ejecute en otra ubicación.

Requisitos

- El host debe encontrarse "Requisitos para el conector".
- 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 necesario de terceros durante la instalación.
- El instalador del conector tiene acceso a varias direcciones URL durante el proceso de instalación. Debe asegurarse de que se permita el acceso saliente a Internet a estos puntos finales:

- 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

  Es posible que el host intente actualizar paquetes de sistema operativo durante la instalación. El host puede ponerse en contacto con diferentes sitios de duplicación para estos paquetes de SO.

Acerca de esta tarea

- No se requieren privilegios de usuario raíz para instalar el conector.
- La instalación 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. El conector 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, el conector se actualiza automáticamente si hay una nueva versión disponible.

Pasos

1. Descargue el software Cloud Manager del "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".

2. Asigne permisos para ejecutar el script.

   ejemplo

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Ejecute el script de instalación:
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent ejecuta la instalación sin solicitar información.

   se requiere *proxy* si el host 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.

3. 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.

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

dos veces si especificó un servidor proxy.

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

   https://ipaddress:port

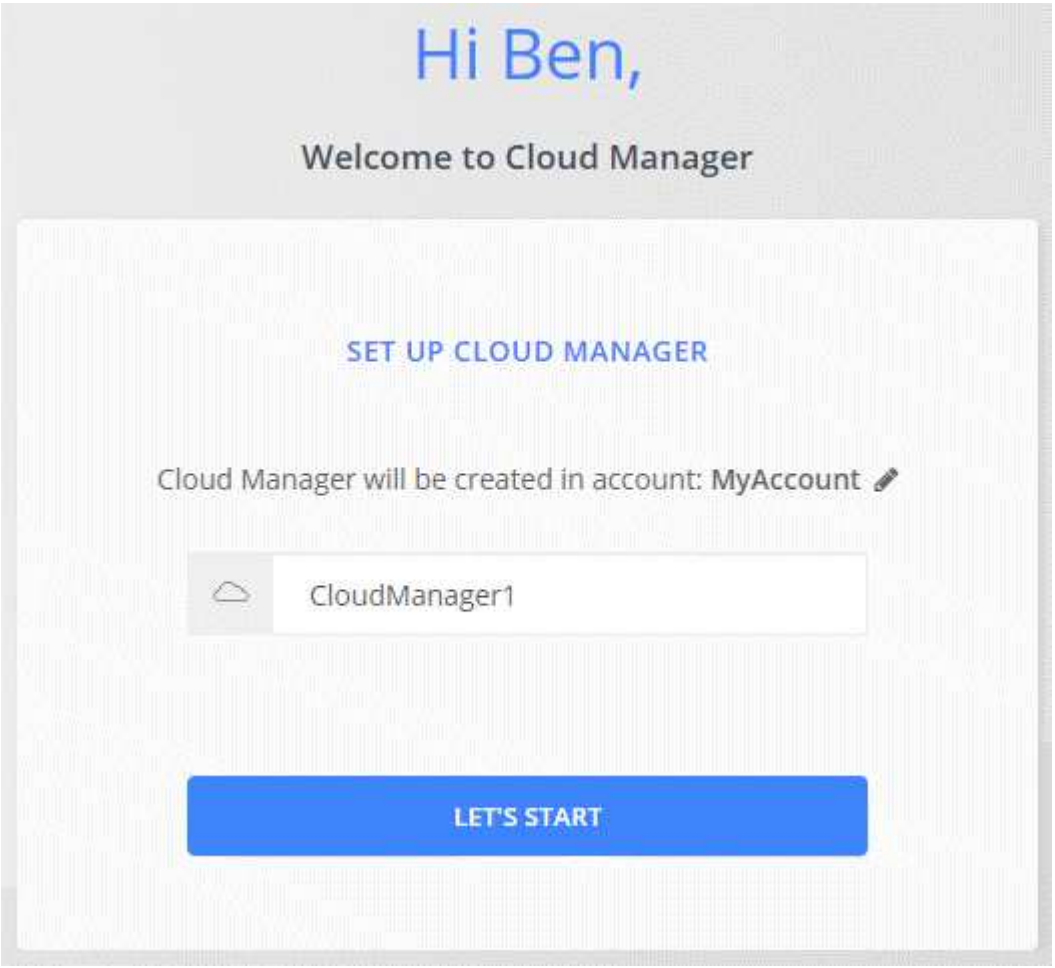
   ipaddress puede ser localhost, una dirección IP privada o una dirección IP pública, dependiendo de la configuración del host. Por ejemplo, si el conector está en la nube pública sin una dirección IP pública, debe introducir una dirección IP privada desde un host que tenga una conexión con el host del conector.

   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

5. Regístrese en NetApp Cloud Central o inicie sesión.
6. Después de iniciar sesión, configure Cloud Manager:
   a. Especifique la cuenta de Cloud Central que desea asociar con el conector.

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

   b. Escriba un nombre para el sistema.



Resultado

El conector ya está instalado y configurado con su cuenta de Cloud Central. Cloud Manager utilizará automáticamente este conector cuando cree nuevos entornos de trabajo.

Después de terminar

Configure permisos para que Cloud Manager pueda gestionar recursos y procesos en su entorno de cloud público:

- 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 del conector".
  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.

Configuración predeterminada del conector

Si necesita solucionar problemas del conector, puede ser útil entender cómo está configurado.

- Si puso en marcha el conector desde Cloud Manager (o directamente desde el mercado de un proveedor de cloud), tenga en cuenta lo siguiente:
  - En AWS, el nombre de usuario de la instancia de EC2 Linux es ec2-user.
  - El sistema operativo de la imagen es el siguiente:
    - AWS: Red Hat Enterprise Linux 7.5 (HVM)
    - Azure: Red Hat Enterprise Linux 7.6 (HVM)
    - GCP: CentOS 7.6

      El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.
- La carpeta de instalación del conector se encuentra en la siguiente ubicación:

  /opt/aplicación/netapp/cloudmanager
- Los archivos de registro se encuentran en la siguiente carpeta:

  /opt/application/netapp/cloudmanager/log
- El servicio Cloud Manager se llama occm.
- El servicio occm depende del servicio MySQL.

  Si el servicio MySQL está inactivo, entonces el servicio occm también está inactivo.
- Cloud Manager instala los siguientes paquetes en el host Linux, si no están ya instalados:

- 7zip
- AWSCLI
- Docker
- Java
- Kubectl
- MySQL
- Tridentctl
- Tire
- Consiga

- El conector utiliza los siguientes puertos en el host Linux:
  - 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
  - 8666 para la API de Service Manager
  - 8777 para la API de servicio de contenedores Health-Checker

Gestionar credenciales

AWS

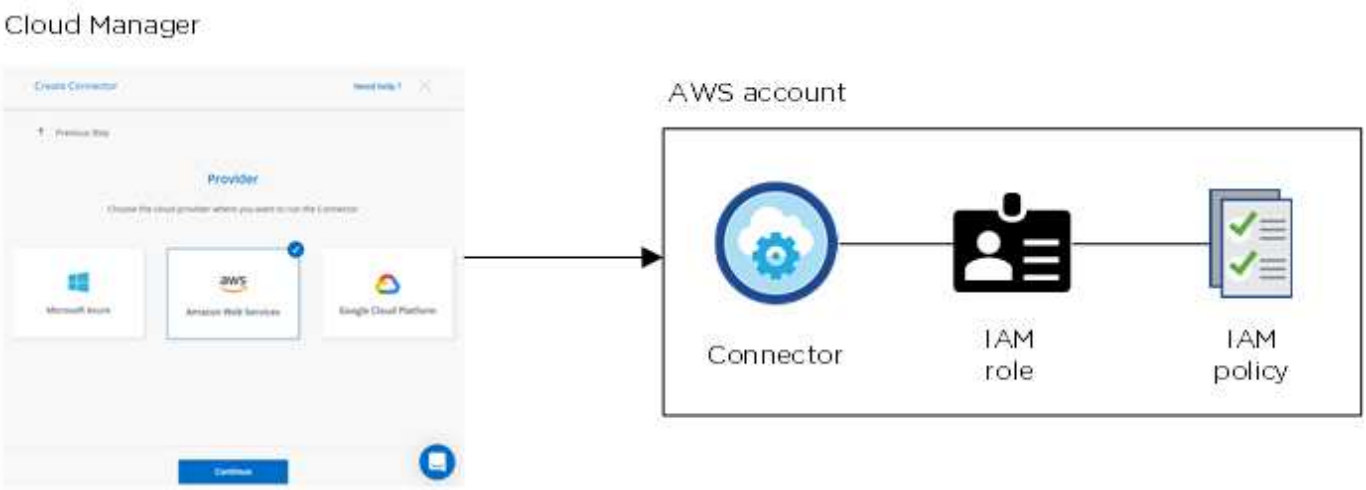
Credenciales y permisos de AWS

Cloud Manager le permite elegir las credenciales de AWS que desea utilizar al implementar Cloud Volumes ONTAP. Puede implementar todos sus sistemas Cloud Volumes ONTAP con las credenciales iniciales de AWS o bien añadir credenciales adicionales.

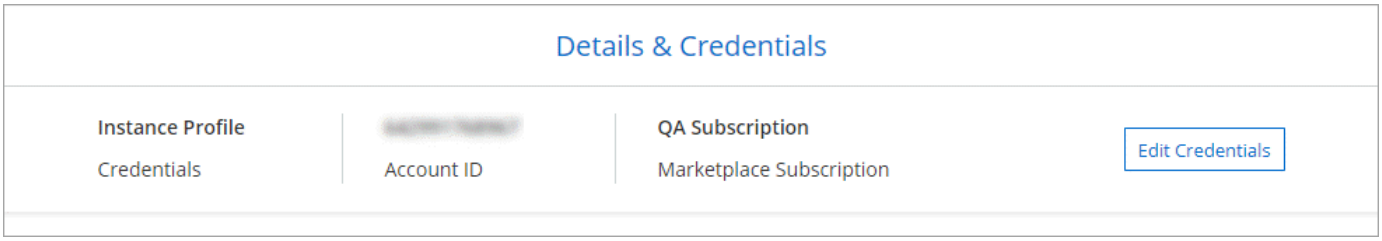
Credenciales iniciales de AWS

Al implementar un conector desde Cloud Manager, necesita utilizar una cuenta de AWS que tenga permisos para ejecutar la instancia de Connector. Los permisos necesarios se enumeran en la "La política de implementación de conectores para AWS".

Cuando Cloud Manager inicia la instancia de Connector en AWS, crea un rol IAM y un perfil de instancia para la instancia. También une una política que ofrece permisos para gestionar recursos y procesos dentro de esa cuenta de AWS. "Revise cómo Cloud Manager utiliza los permisos".

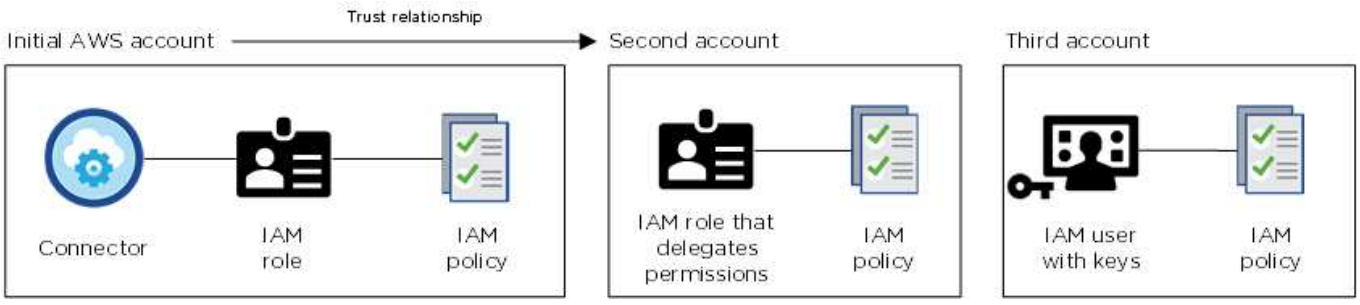


Cloud Manager selecciona estas credenciales de AWS de forma predeterminada al crear un entorno de trabajo nuevo para Cloud Volumes ONTAP:



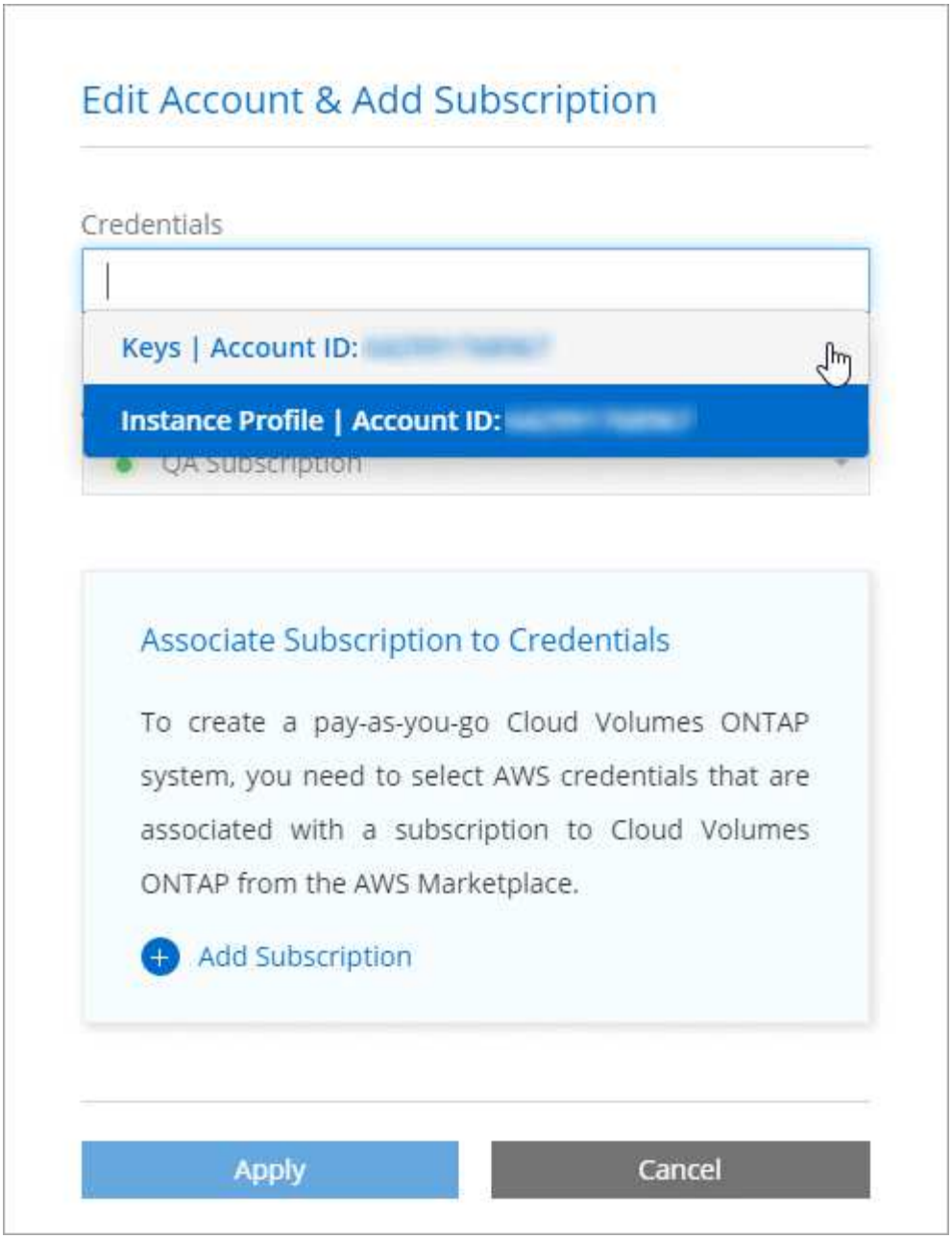
Credenciales adicionales de AWS

Si desea ejecutar Cloud Volumes ONTAP en diferentes cuentas de AWS, puede hacerlo también "Proporcione las claves AWS para un usuario de IAM o el ARN de un rol en una cuenta de confianza". En la siguiente imagen se muestran dos cuentas adicionales, una que proporciona permisos a través de una función IAM en una cuenta de confianza y otra a través de las claves AWS de un usuario de IAM:



Entonces lo haría "Añada las credenciales de la cuenta a Cloud Manager" Especificando el nombre de recurso de Amazon (ARN) del rol de IAM o las claves de AWS del usuario de IAM.

Después de añadir otro conjunto de credenciales, puede cambiar a ellas al crear un nuevo entorno de trabajo:



¿Qué pasa con las puestas en marcha de Marketplace y las puestas en marcha en las instalaciones?

En las secciones anteriores se describe el método de implementación recomendado para el conector, que es de Cloud Manager. También puede implementar un conector en AWS desde el "Mercado AWS" y usted puede "Instale el conector en las instalaciones".

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Solo tiene que crear y configurar manualmente el rol IAM y, a continuación, proporcionar permisos para cualquier cuenta adicional.

En el caso de las implementaciones locales, no se puede configurar la función de IAM para el sistema Cloud Manager, pero se pueden proporcionar permisos del mismo modo que se busca para cuentas de AWS adicionales.

¿Cómo puedo rotar mis credenciales de AWS de forma segura?

Como se ha descrito anteriormente, Cloud Manager permite proporcionar credenciales de AWS de varias

maneras: Una función IAM asociada con la instancia de Connector, asumiendo un rol IAM en una cuenta de confianza o proporcionando claves de acceso de AWS.

Con las dos primeras opciones, Cloud Manager utiliza AWS Security Token Service para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica, es automático y seguro.

Si proporciona claves de acceso a Cloud Manager para AWS, debe rotar las claves se actualizan en Cloud Manager a un intervalo regular. Este es un proceso completamente manual.

Gestión de las credenciales y suscripciones de AWS para Cloud Manager

Al crear un sistema de Cloud Volumes ONTAP, debe seleccionar las credenciales y la suscripción de AWS para utilizarlas con ese sistema. Si administra varias suscripciones de AWS, puede asignar cada una de ellas a diferentes credenciales de AWS desde la página Credentials.

Antes de añadir las credenciales de AWS a Cloud Manager, tiene que proporcionar los permisos necesarios para esa cuenta. Los permisos permiten que Cloud Manager gestione recursos y procesos dentro de esa cuenta de AWS. 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 implementó un conector desde Cloud Manager, Cloud Manager agregó automáticamente credenciales de AWS para la cuenta en la que implementó el conector. Esta cuenta inicial no se agrega si instaló manualmente el software Connector en un sistema existente. "Obtenga más información acerca de los permisos y credenciales de AWS".

opciones

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

¿Cómo puedo rotar mis credenciales de AWS de forma segura?

Cloud Manager le permite proporcionar credenciales de AWS de varias maneras: Una función IAM asociada con la instancia de Connector, asumiendo un rol IAM en una cuenta de confianza o proporcionando claves de acceso de AWS. "Obtenga más información acerca de las credenciales y permisos de AWS".

Con las dos primeras opciones, Cloud Manager utiliza AWS Security Token Service para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica, es automático y seguro.

Si proporciona claves de acceso a Cloud Manager para AWS, debe rotar las claves se actualizan en Cloud Manager a un intervalo regular. Este es un proceso completamente manual.

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

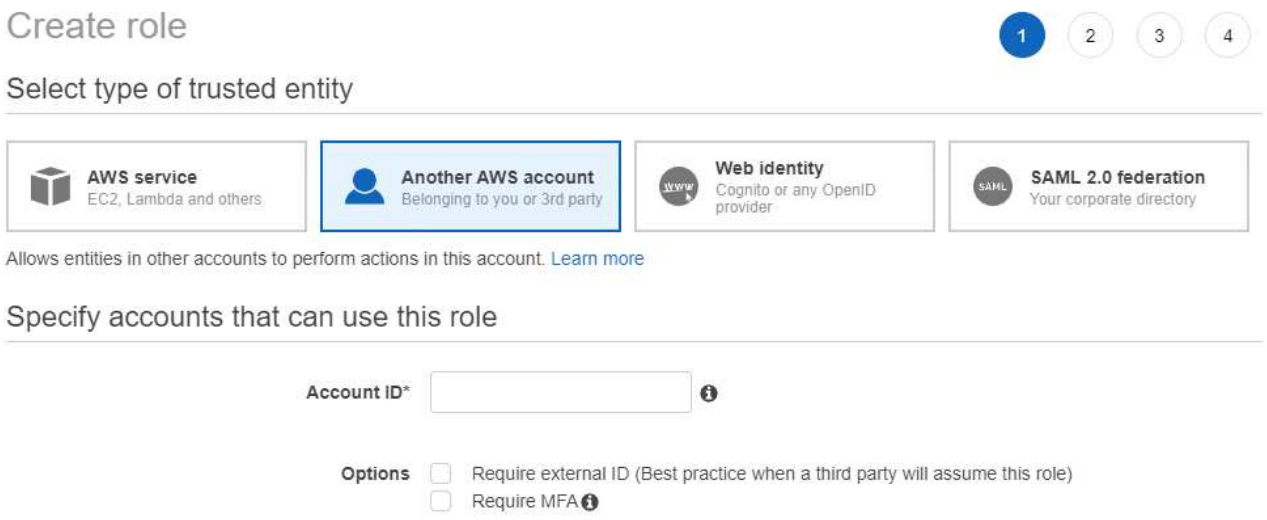
Puede configurar una relación de confianza entre la cuenta AWS de origen en la que ha implementado la instancia de Connector y otras cuentas de AWS mediante los roles IAM. A continuación, debe proporcionar a Cloud Manager el ARN de las funciones de IAM de las cuentas de confianza.

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 código de la cuenta en la que reside la instancia de Connector.
   - Adjunte la política IAM de Cloud Manager, que está disponible en la "Directivas de Cloud Manager".



2. Vaya a la cuenta de origen en la que se encuentra la instancia de Connector y seleccione la función IAM asociada a la instancia.

   a. Haga clic en **Adjuntar directivas** y, a continuación, en **Crear directiva**.

   b. Cree una directiva que incluya la acción "sts:AssumeRole" y el ARN del rol 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

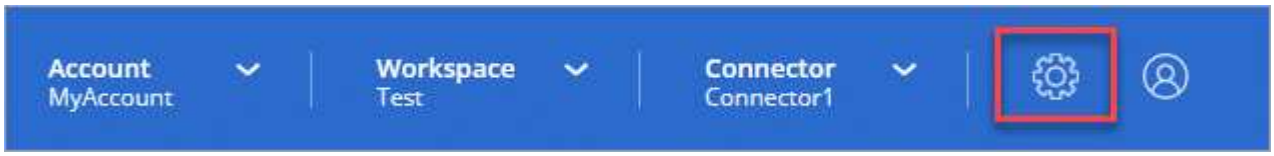
La cuenta ahora tiene los permisos necesarios. Ahora puede añadirlo a Cloud Manager.

Adición de credenciales de AWS a Cloud Manager

Después de proporcionar una cuenta de AWS con los permisos requeridos, puede añadir las credenciales para dicha 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 **credenciales**.



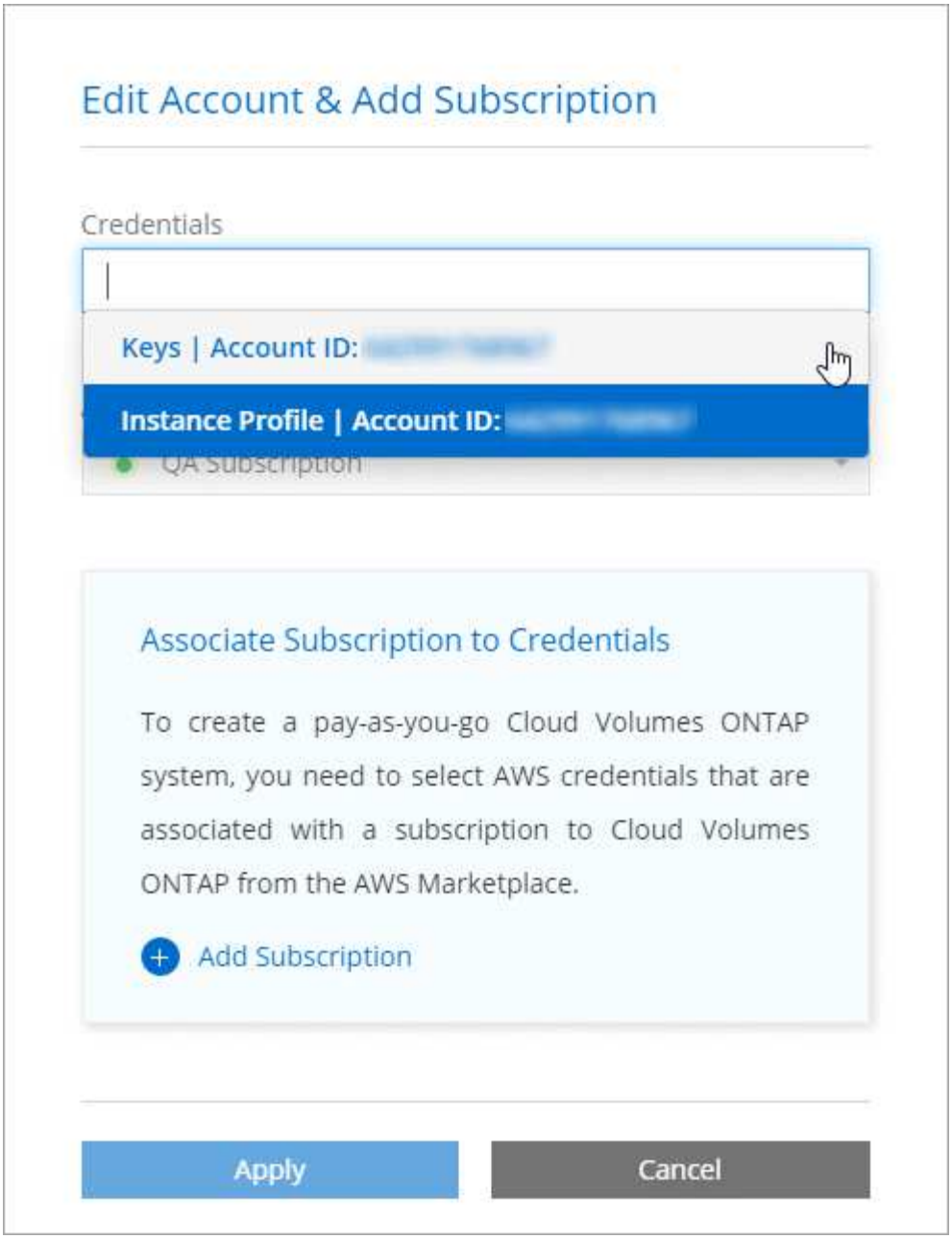
2. Haga clic en **Agregar credenciales** y seleccione **AWS**.
3. Proporcione las claves AWS o el ARN del rol de IAM de confianza.
4. Confirme que se han cumplido los requisitos de la directiva y haga clic en **continuar**.
5. Elija la suscripción de pago por uso que desee asociar con las credenciales o haga clic en **Agregar suscripción** si aún no tiene una.

   Para crear un sistema Cloud Volumes ONTAP de pago por uso, las credenciales de AWS deben estar asociadas con una suscripción a Cloud Volumes ONTAP desde AWS Marketplace.

6. Haga clic en **Agregar**.

Resultado

Ahora puede cambiar a un conjunto de credenciales diferente de la página Details y Credentials al crear un nuevo entorno de trabajo:



Asociación de una suscripción de AWS a credenciales

Después de añadir sus credenciales de AWS a Cloud Manager, puede asociar una suscripción a AWS Marketplace con estas credenciales. La suscripción le permite crear un sistema de pago por uso Cloud Volumes ONTAP y usar otros servicios cloud de NetApp.

Hay dos escenarios en los que puede asociar una suscripción a AWS Marketplace después de haber añadido las credenciales a Cloud Manager:

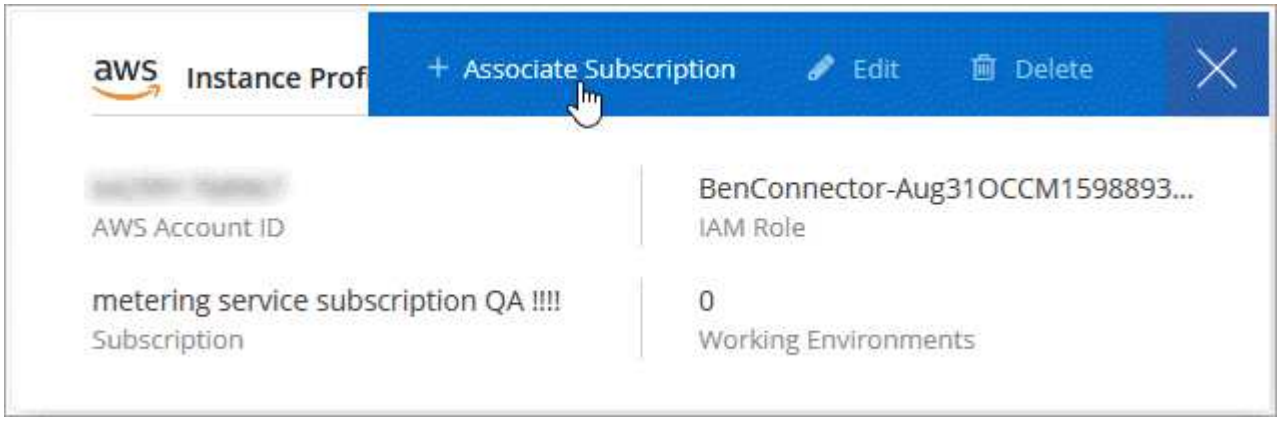
- No asoció una suscripción al agregar inicialmente las credenciales a Cloud Manager.
- Desea sustituir una suscripción existente de AWS Marketplace por una nueva suscripción.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Pase el ratón sobre un conjunto de credenciales y haga clic en el menú de acciones.
3. En el menú, haga clic en **Suscripción asociada**.



4. Seleccione una suscripción de la lista desplegable o haga clic en **Agregar suscripción** y siga los pasos para crear una nueva suscripción.

   ► https://docs.netapp.com/es-es/occm38//media/video_subscribing_aws.mp4 *(video)*

Azure

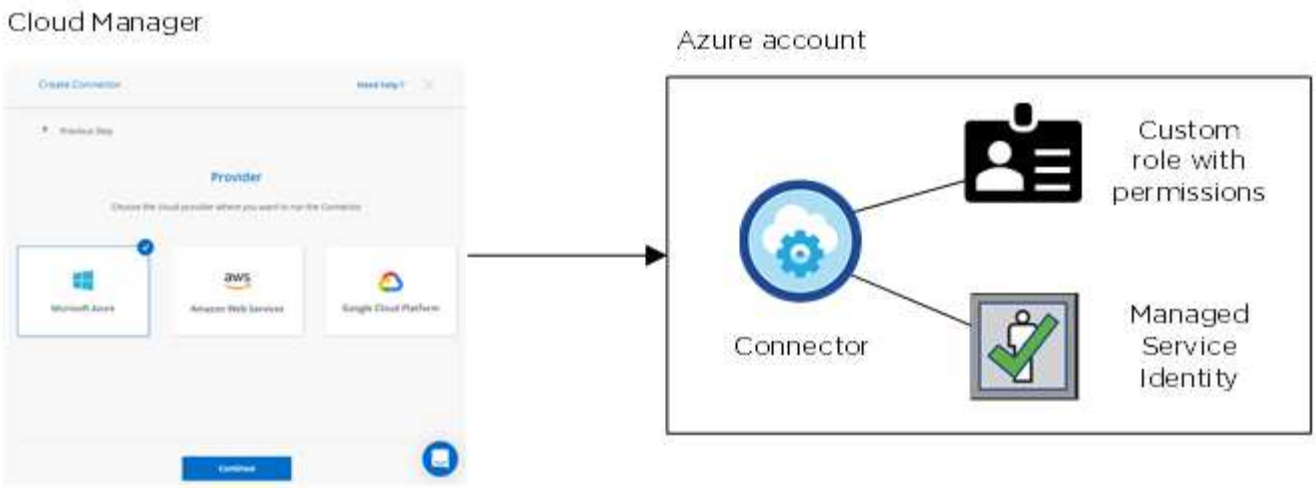
Credenciales y permisos de Azure

Cloud Manager permite elegir las credenciales de Azure que se utilizarán al implementar Cloud Volumes ONTAP. Puede poner en marcha todos los sistemas de Cloud Volumes ONTAP con las credenciales iniciales de Azure o bien añadir credenciales adicionales.

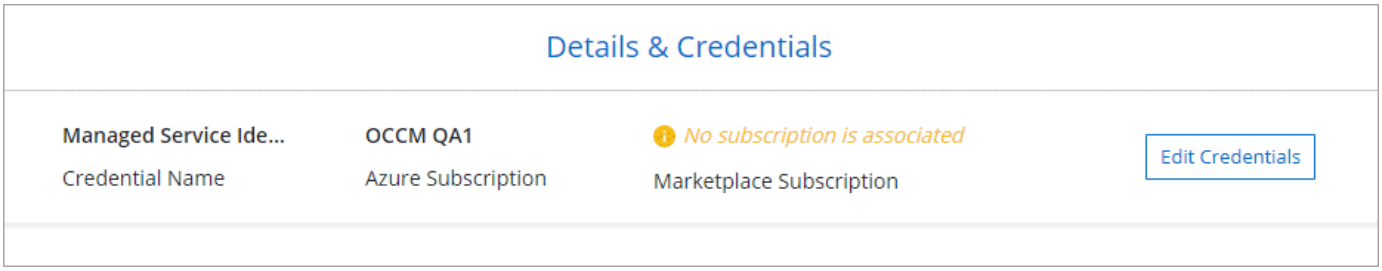
Credenciales iniciales de Azure

Al implementar un conector desde Cloud Manager, necesita utilizar una cuenta de Azure que tenga permisos para implementar la máquina virtual Connector. Los permisos necesarios se enumeran en la "Política de implementación de conectores para Azure".

Cuando Cloud Manager implementa la máquina virtual Connector en Azure, habilita una "identidad administrada asignada por el sistema" en una máquina virtual, crea un rol personalizado y lo asigna a la máquina virtual. El rol proporciona permisos a Cloud Manager para gestionar recursos y procesos dentro de esa suscripción de Azure. "Revise cómo Cloud Manager utiliza los permisos".



Cloud Manager selecciona estas credenciales de Azure de forma predeterminada cuando crea un entorno de trabajo nuevo para Cloud Volumes ONTAP:

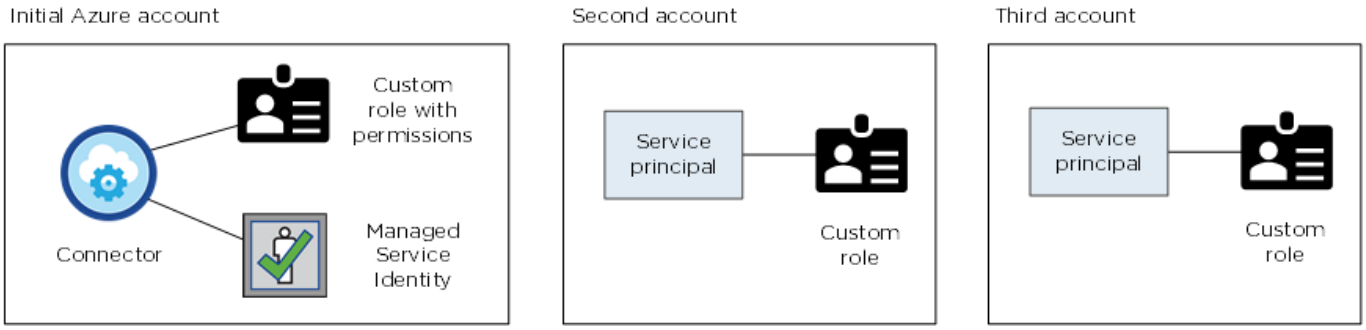


Suscripciones adicionales de Azure para una identidad gestionada

La identidad administrada está asociada a la suscripción en la que inició el conector. Si desea seleccionar una suscripción de Azure diferente, tendrá que hacerlo "asocie la identidad administrada a esas suscripciones".

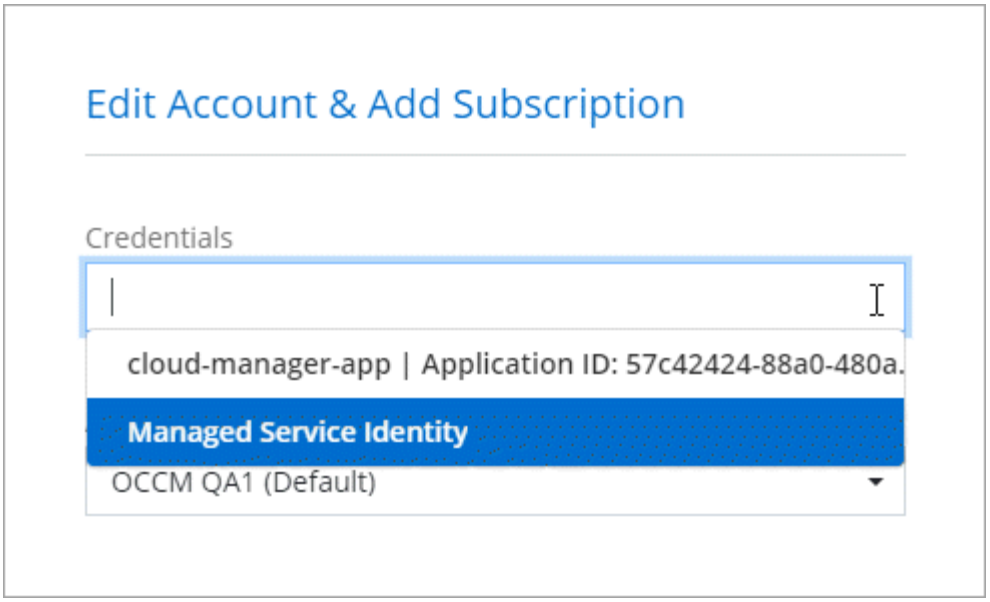
Credenciales adicionales de Azure

Si desea implementar Cloud Volumes ONTAP con diferentes credenciales de Azure, debe conceder los permisos necesarios mediante "Crear y configurar un servicio principal en Azure Active Directorio" Para cada cuenta de Azure. La siguiente imagen muestra dos cuentas adicionales, cada una configurada con una función personalizada y principal de servicio que proporciona permisos:



Entonces lo haría "Añada las credenciales de la cuenta a Cloud Manager" Proporcionando detalles acerca del director de servicio de AD.

Después de añadir otro conjunto de credenciales, puede cambiar a ellas al crear un nuevo entorno de trabajo:



¿Qué pasa con las puestas en marcha de Marketplace y las puestas en marcha en las instalaciones?

En las secciones anteriores se describe el método de puesta en marcha recomendado para el conector, que es de NetApp Cloud Central. También puede implementar un conector en Azure desde "Azure Marketplace", y usted puede "Instale el conector en las instalaciones".

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Sólo tiene que crear y configurar manualmente la identidad administrada para el conector y, a continuación, proporcionar permisos para cualquier cuenta adicional.

Para implementaciones en las instalaciones, no puede configurar una identidad administrada para el conector, pero puede proporcionar permisos como lo haría para cuentas adicionales utilizando un director de servicio.

Administrar credenciales y suscripciones de Azure para Cloud Manager

Al crear un sistema Cloud Volumes ONTAP, necesita seleccionar las credenciales de Azure y la suscripción a Marketplace para utilizar con ese sistema. Si gestiona varias suscripciones a Azure Marketplace, puede asignar cada una de ellas a diferentes credenciales de Azure desde la página Credentials.

Existen dos formas de gestionar las credenciales de Azure en Cloud Manager. En primer lugar, si desea implementar Cloud Volumes ONTAP en diferentes cuentas de Azure, tendrá que proporcionar los permisos necesarios y añadir las credenciales a Cloud Manager. La segunda es asociar suscripciones adicionales a la identidad administrada de Azure.

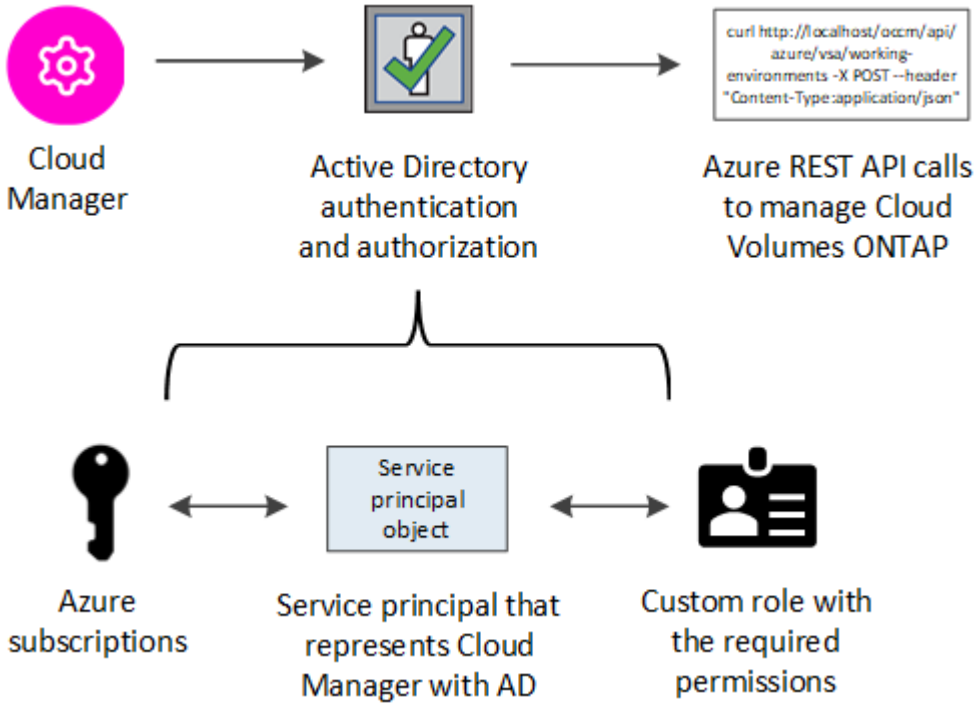
Cuando implementa un conector desde Cloud Manager, Cloud Manager agrega automáticamente la cuenta de Azure en la que implementó Connector. No se agrega una cuenta inicial si instaló manualmente el software Connector en un sistema existente. "Obtenga más información acerca de las cuentas y los permisos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

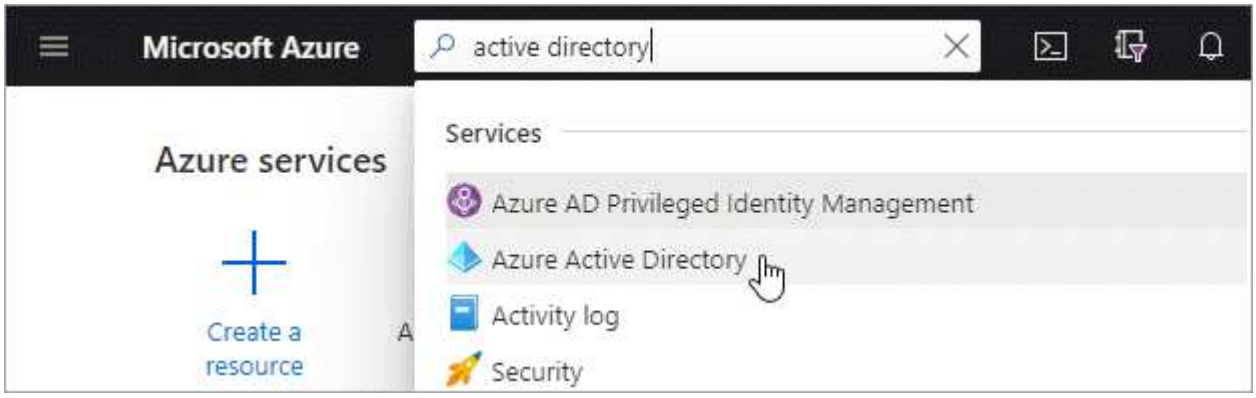
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que Cloud Manager pueda usar para el control de acceso basado en roles.

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_3.8.7.json
```

Ahora debe tener una función personalizada denominada *Cloud Manager Operator*.

2. Asigne la aplicación al rol:

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

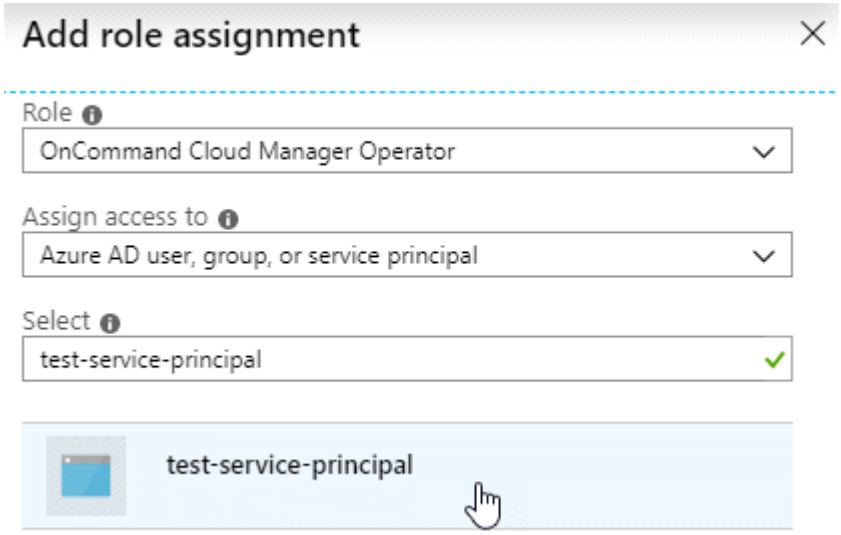
   b. Seleccione la suscripción.

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

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

   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.

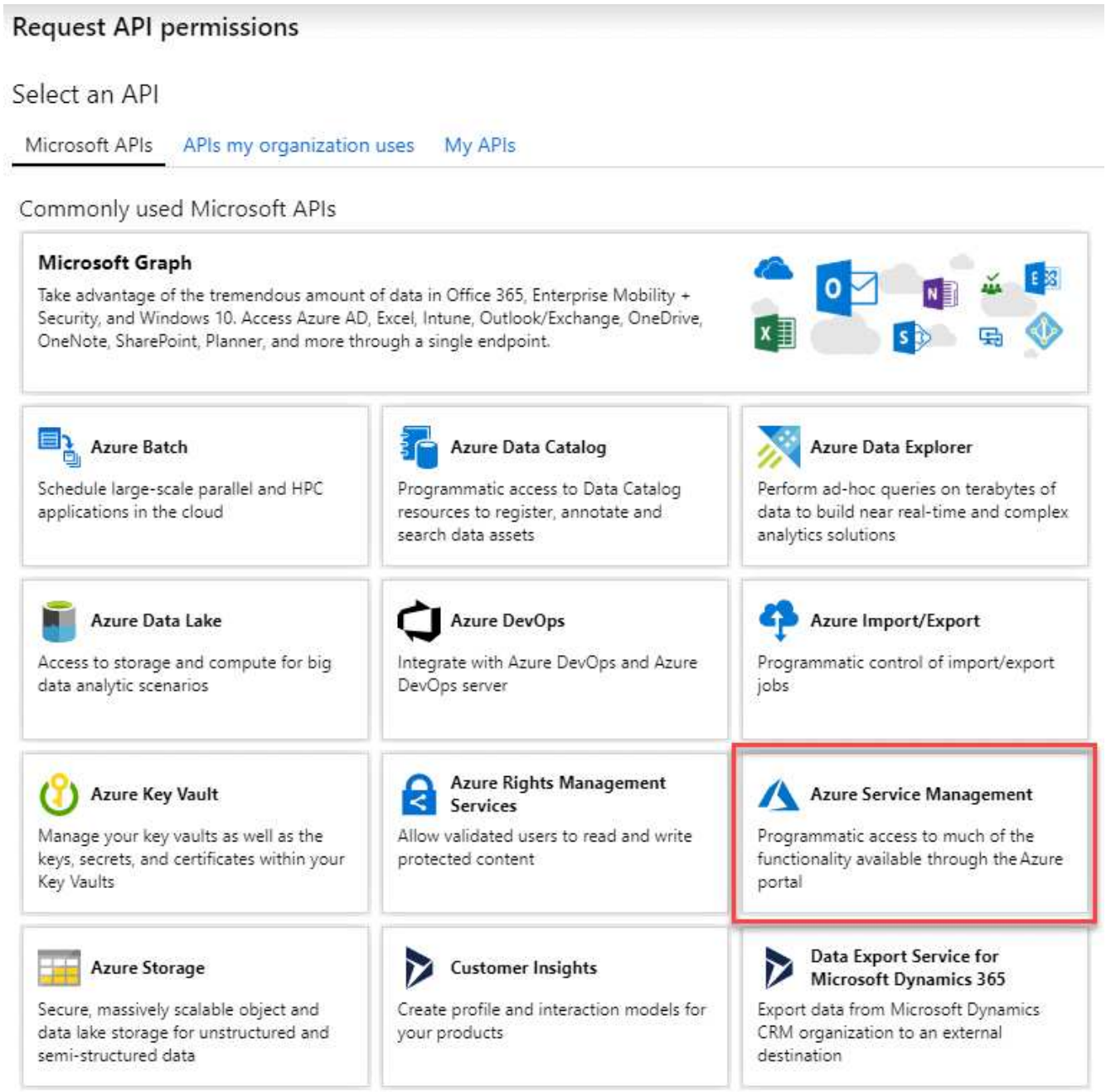
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. Cloud Manager le permite seleccionar la suscripción que desea utilizar al poner en marcha Cloud Volumes ONTAP.

Agregar permisos de API de administración de servicios de Windows Azure

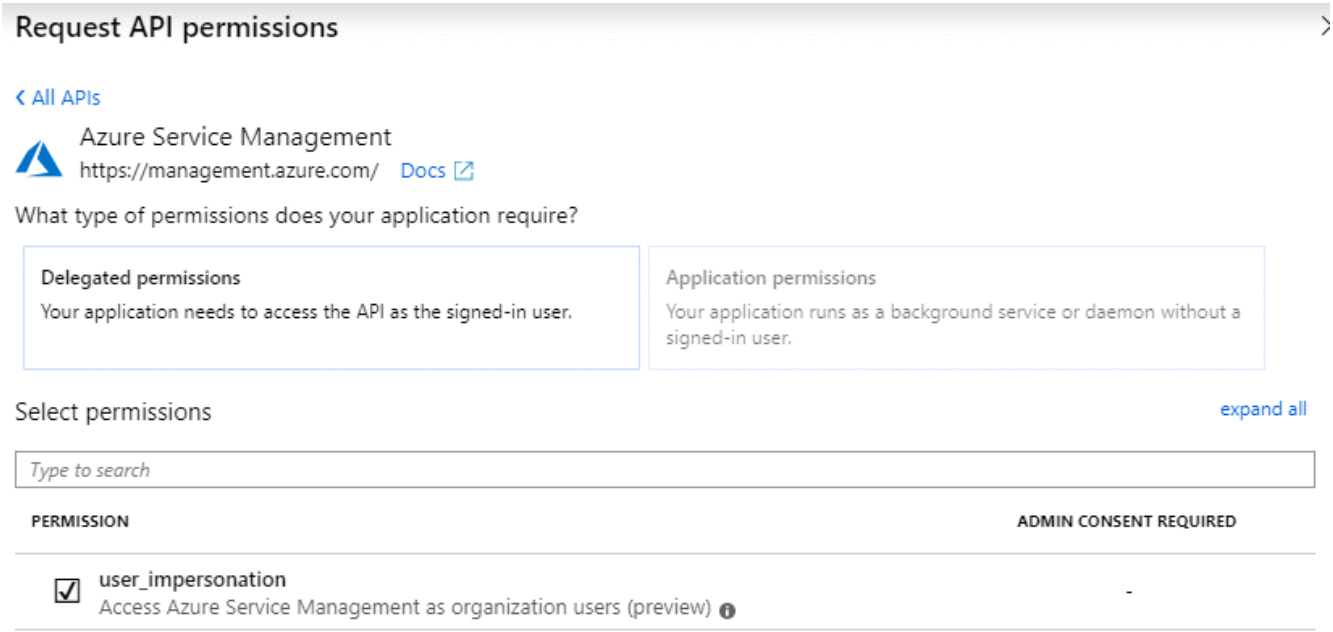
El principal de servicio debe tener permisos de "API de administración de servicios de Windows Azure".

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**.

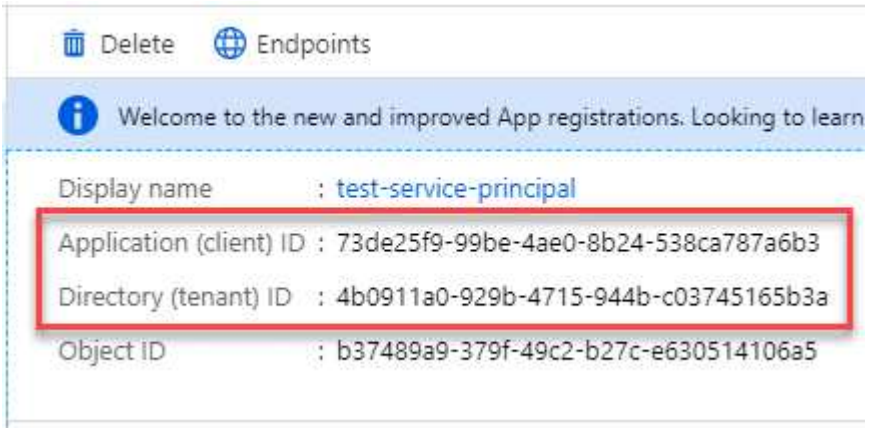


Obteniendo el ID de aplicación y el ID de directorio

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.

Añadir credenciales de Azure a Cloud Manager

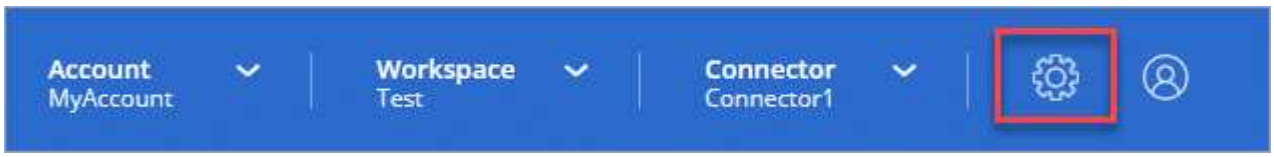
Después de proporcionar una cuenta de Azure con los permisos requeridos, puede añadir las credenciales para esa cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

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



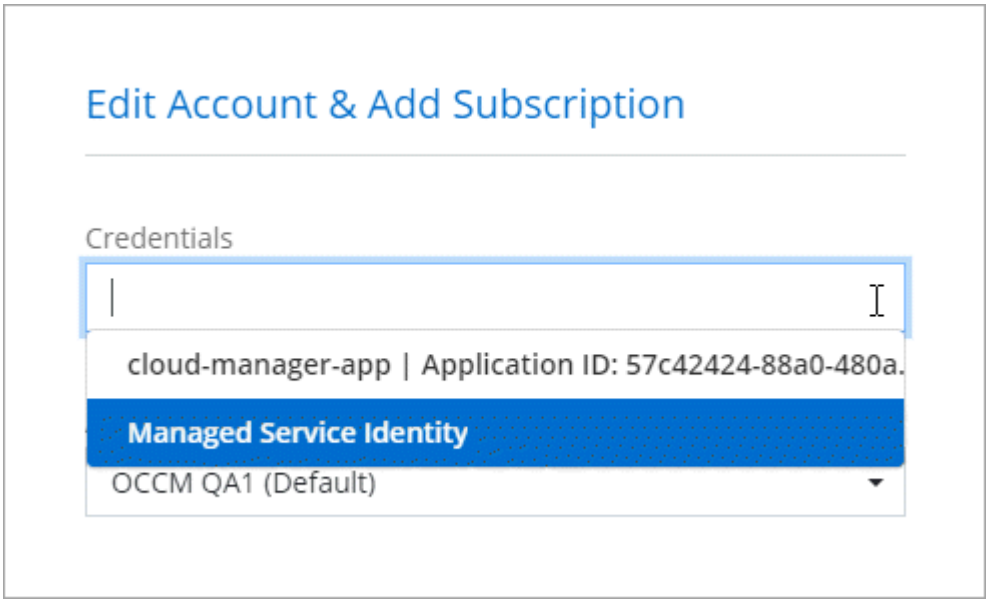
2. Haga clic en **Agregar credenciales** y seleccione **Microsoft Azure**.
3. Introduzca la información acerca del director del servicio de Azure Active Directory que otorga los permisos necesarios:
   - ID de aplicación (cliente): Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - ID de directorio (arrendatario): Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - Client Secret: Consulte Crear un secreto de cliente.
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **continuar**.
5. Elija la suscripción de pago por uso que desee asociar con las credenciales o haga clic en **Agregar suscripción** si aún no tiene una.

Para crear un sistema de Cloud Volumes ONTAP de pago por uso, las credenciales de Azure deben estar asociadas con una suscripción a Cloud Volumes ONTAP desde Azure Marketplace.

6. Haga clic en **Agregar**.

Resultado

Ahora puede cambiar a un conjunto diferente de credenciales La página Details y Credentials "al crear un nuevo entorno de trabajo":



Asociación de una suscripción de Azure Marketplace a credenciales

Después de añadir sus credenciales de Azure a Cloud Manager, puede asociar una suscripción de Azure Marketplace a esas credenciales. La suscripción le permite crear un sistema de pago por uso Cloud Volumes ONTAP y usar otros servicios cloud de NetApp.

Hay dos escenarios en los que puede asociar una suscripción a Azure Marketplace después de haber añadido las credenciales a Cloud Manager:

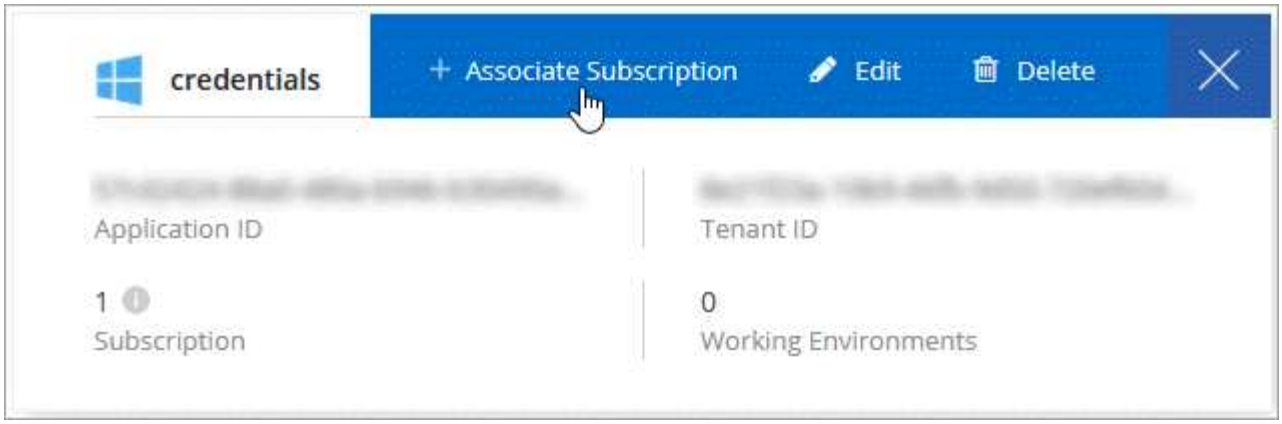
- No asoció una suscripción al agregar inicialmente las credenciales a Cloud Manager.
- Desea sustituir una suscripción existente de Azure Marketplace por una nueva suscripción.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Pase el ratón sobre un conjunto de credenciales y haga clic en el menú de acciones.
3. En el menú, haga clic en **Suscripción asociada**.



4. Seleccione una suscripción de la lista desplegable o haga clic en **Agregar suscripción** y siga los pasos para crear una nueva suscripción.

   El siguiente vídeo se inicia desde el contexto del asistente de entorno de trabajo, pero muestra el mismo flujo de trabajo después de hacer clic en **Agregar suscripción**:

   ► https://docs.netapp.com/es-es/occm38//media/video_subscribing_azure.mp4 *(video)*

Asociar suscripciones de Azure adicionales a una identidad administrada

Cloud Manager le permite elegir las credenciales de Azure y la suscripción a Azure en la que desea 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" Al implementar un conector desde Cloud Manager. Cuando implementó el conector, Cloud Manager creó el rol de operador de Cloud Manager y lo asignó a la máquina virtual Connector.

Pasos

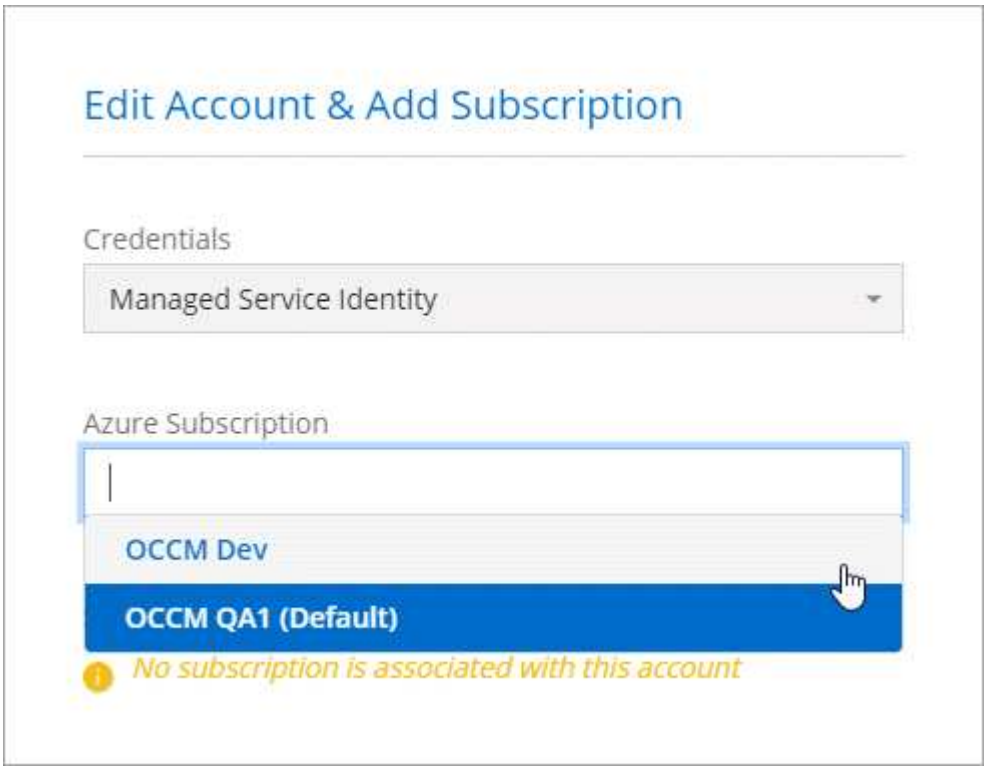
1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar Cloud Volumes ONTAP.
3. Haga clic en **Control de acceso (IAM)**.
   a. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos: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

        Es el nombre predeterminado que se proporciona en la "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 Connector.
      - Seleccione la máquina virtual conector.
      - 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.



GCP

Proyectos, permisos y cuentas de Google Cloud

Una cuenta de servicio proporciona a Cloud Manager permisos para implementar y gestionar sistemas de Cloud Volumes ONTAP en el mismo proyecto que Cloud Manager o en diferentes proyectos.

Proyecto y permisos para Cloud Manager

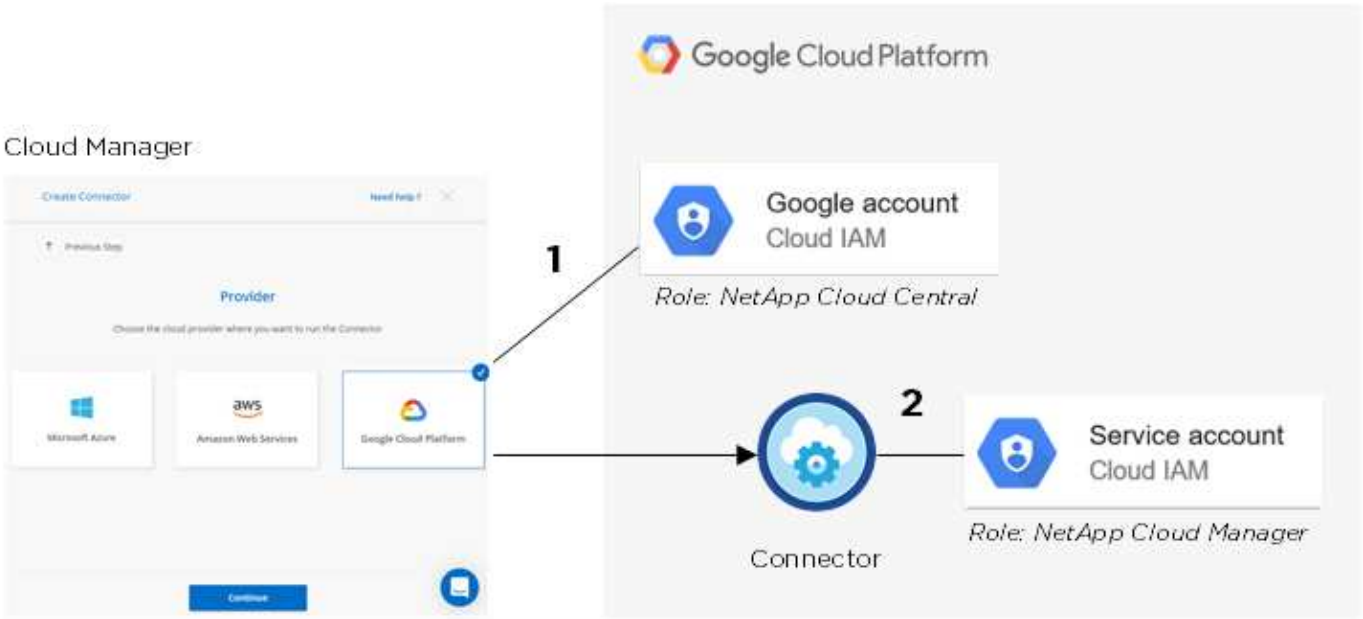
Antes de poder poner en marcha Cloud Volumes ONTAP en Google Cloud, primero debe poner en marcha un conector en un proyecto de Google Cloud. El conector no puede ejecutarse en sus instalaciones ni en un proveedor de cloud diferente.

Debe haber dos conjuntos de permisos antes de implementar un conector directamente desde Cloud Manager:

1. Necesita implementar un conector con una cuenta de Google que tenga permisos para iniciar la instancia de Connector VM desde Cloud Manager.
2. Al desplegar el conector, se le pedirá que seleccione un "cuenta de servicio" Para la instancia de máquina virtual. Cloud Manager obtiene permisos de la cuenta de servicio para crear y gestionar sistemas de Cloud Volumes ONTAP en su nombre. Los permisos se proporcionan asociando una función personalizada a la cuenta de servicio.

Hemos configurado dos archivos YAML que incluyen los permisos necesarios para el usuario y la cuenta de servicio. "Aprenda a usar los archivos YAML para configurar permisos".

La siguiente imagen muestra los requisitos de permisos descritos en los números 1 y 2 anteriores:



Proyecto para Cloud Volumes ONTAP

Cloud Volumes ONTAP puede residir en el mismo proyecto que el conector o en un proyecto diferente. Para implementar Cloud Volumes ONTAP en un proyecto diferente, primero debe agregar la cuenta de servicio del conector y la función a ese proyecto.

- "Aprenda a configurar una cuenta de servicio (consulte el paso 2).".
- "Descubra cómo implementar Cloud Volumes ONTAP en GCP y seleccione un proyecto".

Responsables de la organización en niveles de los datos

Cloud Manager requiere una cuenta de GCP para Cloud Volumes ONTAP 9.6, pero no para la versión 9.7 ni para las posteriores. Si desea utilizar la organización en niveles de datos con Cloud Volumes ONTAP 9.7, siga el paso 4 en "Introducción a Cloud Volumes ONTAP en Google Cloud Platform".

Es necesario añadir una cuenta de Google Cloud a Cloud Manager para habilitar la organización en niveles de datos en un sistema Cloud Volumes ONTAP 9.6. Organización en niveles de datos organiza automáticamente en niveles los datos fríos en un almacenamiento de objetos de bajo coste, lo que le permite recuperar espacio en el almacenamiento principal y reducir el almacenamiento secundario.

Al añadir la cuenta, necesita 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.

Después de añadir una cuenta de Google Cloud, podrá habilitar la organización en niveles de los datos en volúmenes individuales al crearlos, modificarlos o replicarlos.

- "Aprenda a configurar y añadir cuentas de GCP a. Cloud Manager".
- "Aprenda a organizar en niveles los datos inactivos en almacenamiento de objetos de bajo coste".

Gestión de credenciales y suscripciones de GCP para Cloud Manager

Puede gestionar dos tipos de credenciales de Google Cloud Platform desde Cloud Manager: Las credenciales asociadas con la instancia de Connector VM y las claves de acceso al almacenamiento utilizadas con un sistema Cloud Volumes ONTAP 9.6 para "organización en niveles de los datos".

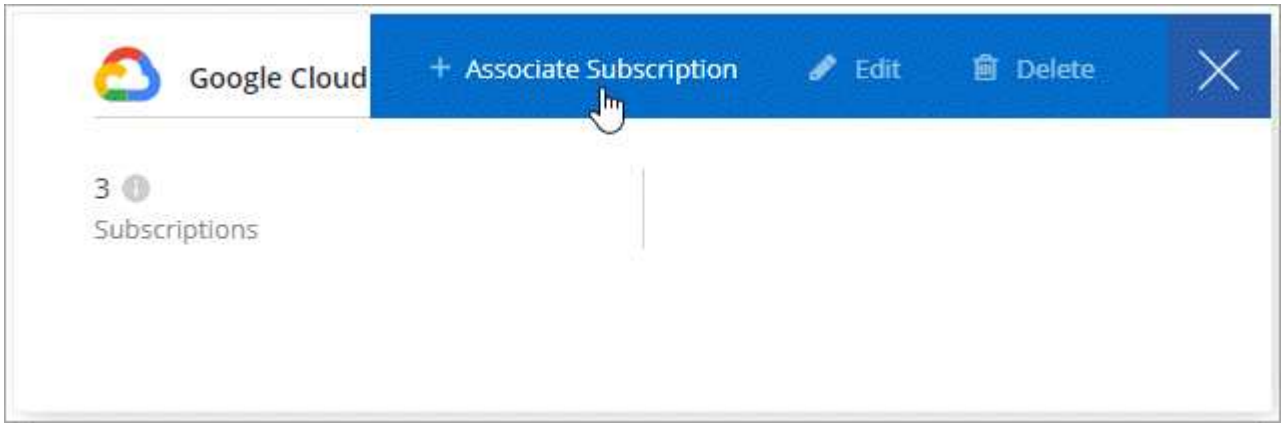
Asociación de una suscripción a Marketplace con credenciales de GCP

Al implementar un conector en GCP, Cloud Manager crea un conjunto predeterminado de credenciales asociadas con la instancia de Connector VM. Estas son las credenciales que utiliza Cloud Manager para poner en marcha Cloud Volumes ONTAP.

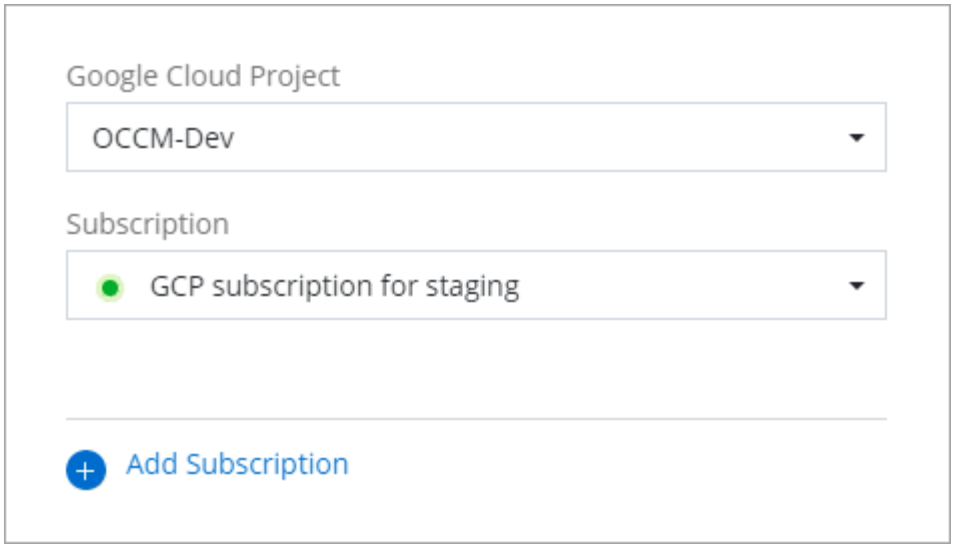
En cualquier momento, puede cambiar la suscripción de Marketplace asociada a estas credenciales. La suscripción le permite crear un sistema de pago por uso Cloud Volumes ONTAP y usar otros servicios cloud de NetApp.

Pasos

1. En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **credenciales**.
2. Pase el ratón sobre un conjunto de credenciales y haga clic en el menú de acciones.
3. En el menú, haga clic en **Suscripción asociada**.



4. Seleccione un proyecto de Google Cloud y una suscripción en la lista desplegable o haga clic en **Agregar suscripción** y siga los pasos para crear una nueva suscripción.



5. Haga clic en **asociar**.

Configuración y adición de cuentas de GCP para la organización de datos en niveles con Cloud Volumes ONTAP 9.6

Si desea habilitar una instancia de Cloud Volumes ONTAP 9.6 sistema para "organización en niveles de los datos", debe proporcionar a Cloud Manager una clave de acceso a almacenamiento para una cuenta de servicio que tenga 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.

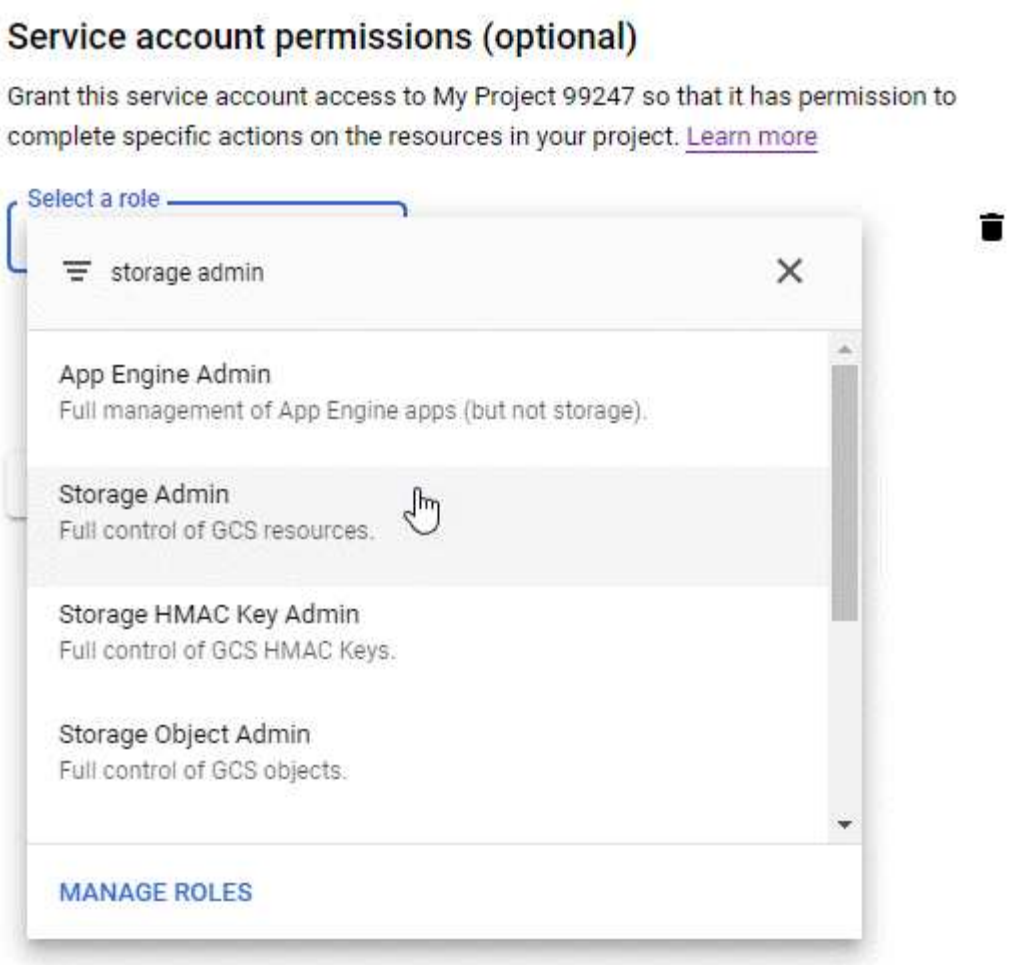
Si desea utilizar la organización en niveles de datos con Cloud Volumes ONTAP 9.7, siga el paso 4 en "Introducción a Cloud Volumes ONTAP en Google Cloud Platform".

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

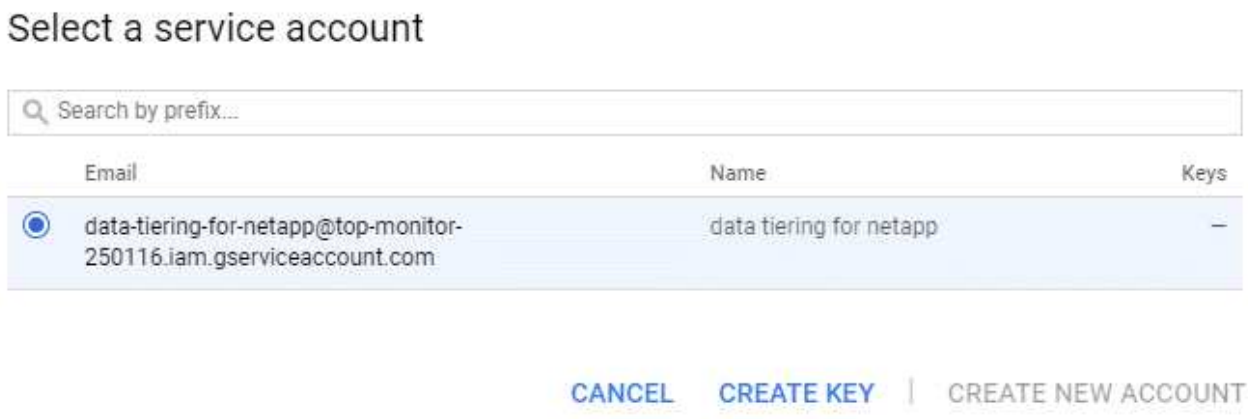
Una cuenta de servicio permite que Cloud Manager autentique y acceda a los bloques de almacenamiento en cloud que se utilizan para la organización en niveles de los datos. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

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

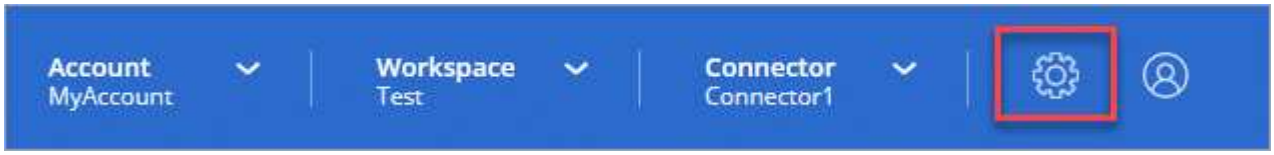
Ahora que tiene una clave de acceso para una cuenta de servicio, puede agregarla a Cloud Manager.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

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



2. Haga clic en **Agregar credenciales** y seleccione **Google Cloud**.
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 en un sistema Cloud Volumes ONTAP 9.6 cuando los crea, modifica o replica. 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.

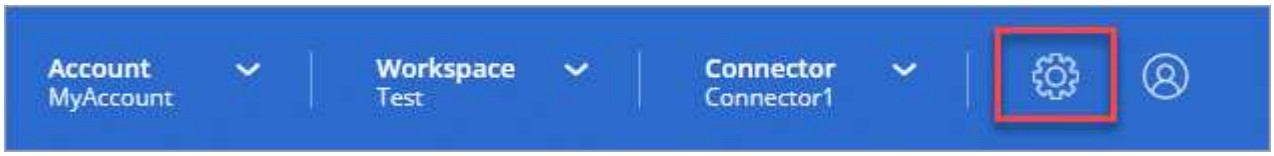
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

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 **credenciales**.



3. Haga clic en **Add Credentials** 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"

Gestión de usuarios, áreas de trabajo, conectores y suscripciones

"Después de realizar la configuración inicial", es posible que necesite administrar la configuración de su cuenta más adelante mediante la administración de usuarios, áreas de trabajo, conectores y suscripciones.

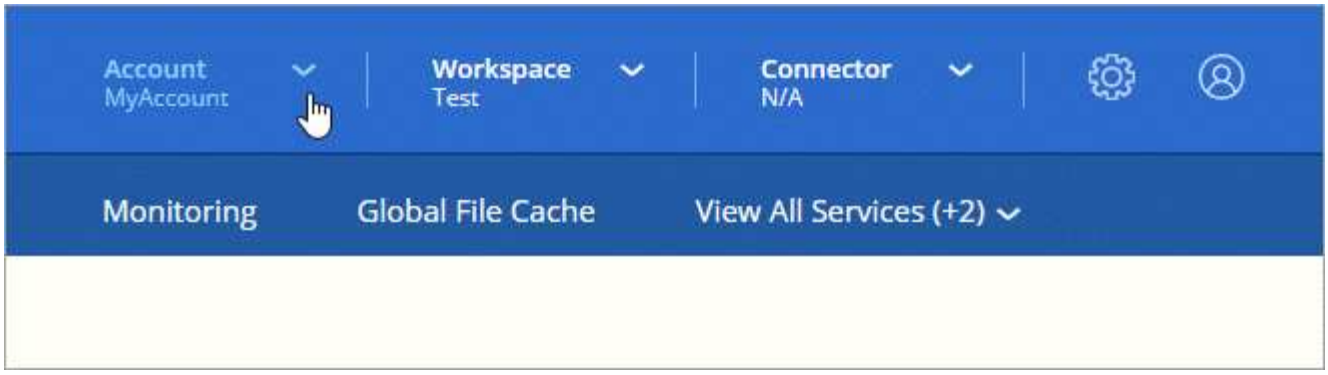
"Obtenga más información sobre cómo funcionan las cuentas de Cloud Central".

Adición de usuarios

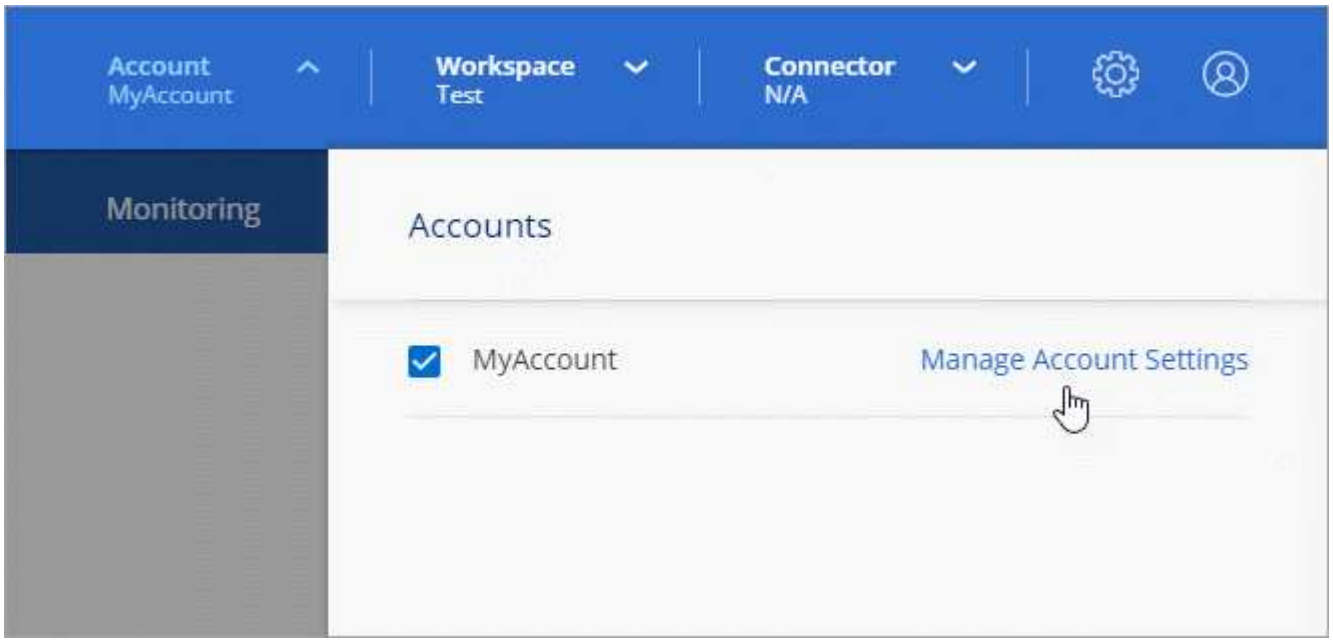
Asocie los usuarios de Cloud Central a la cuenta de Cloud Central para que esos usuarios puedan crear y gestionar entornos de trabajo en Cloud Manager.

Pasos

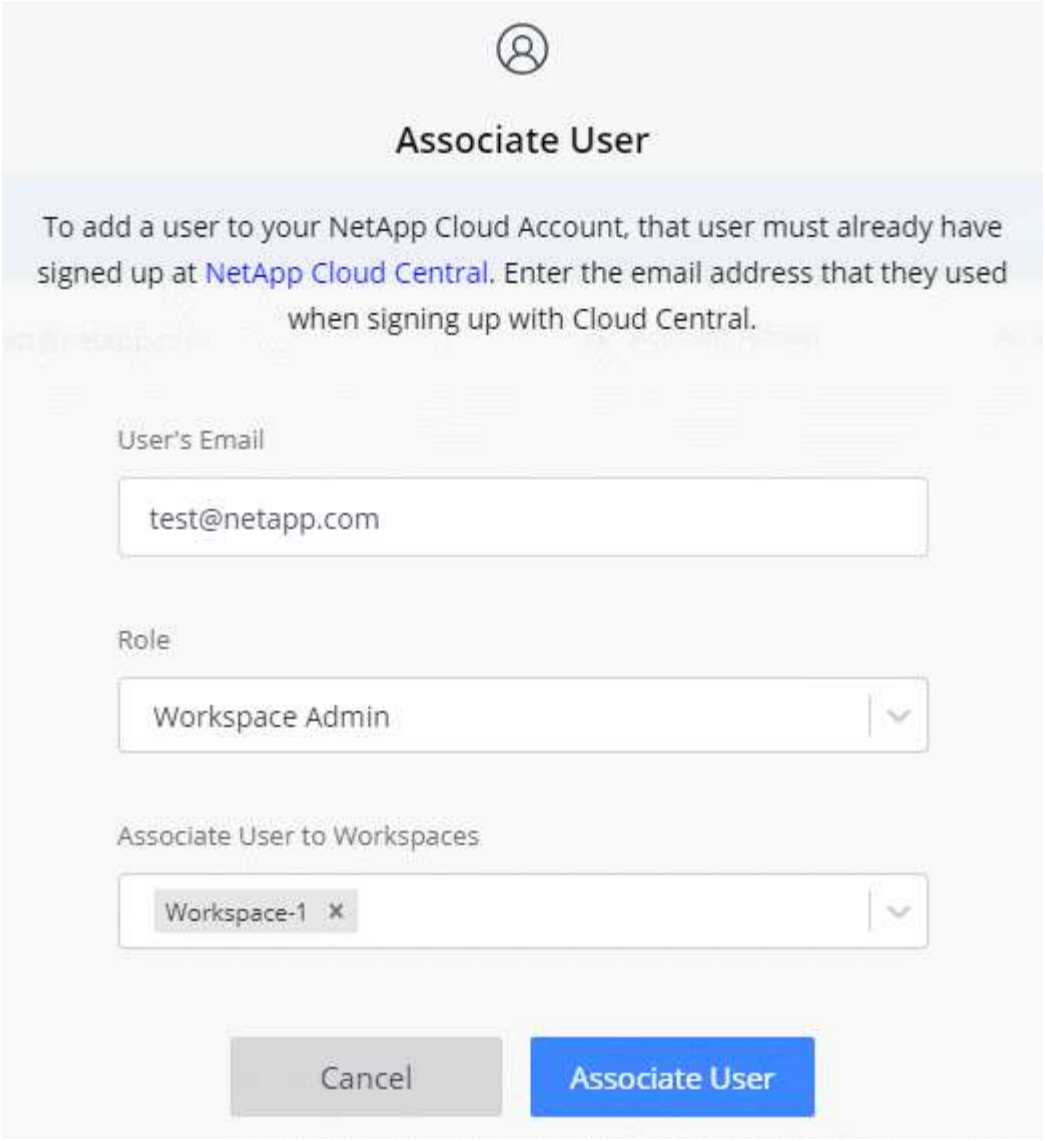
1. Si el usuario aún no lo ha hecho, pida al usuario que vaya a. "Cloud Central de NetApp" y regístrese.
2. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta**.



3. Haga clic en **Administrar cuenta** junto a la cuenta seleccionada actualmente.



4. En la ficha usuarios, haga clic en **Usuario asociado**.
5. 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.
   - **Visor de cumplimiento**: Sólo puede ver información de cumplimiento y generar informes para áreas de trabajo a las que tienen permiso para acceder.
6. Si ha seleccionado Administrador de área de trabajo o Visor de cumplimiento, seleccione uno o varios espacios de trabajo para asociarlos con ese usuario.



7. Haga clic en **Usuario asociado**.

Resultado

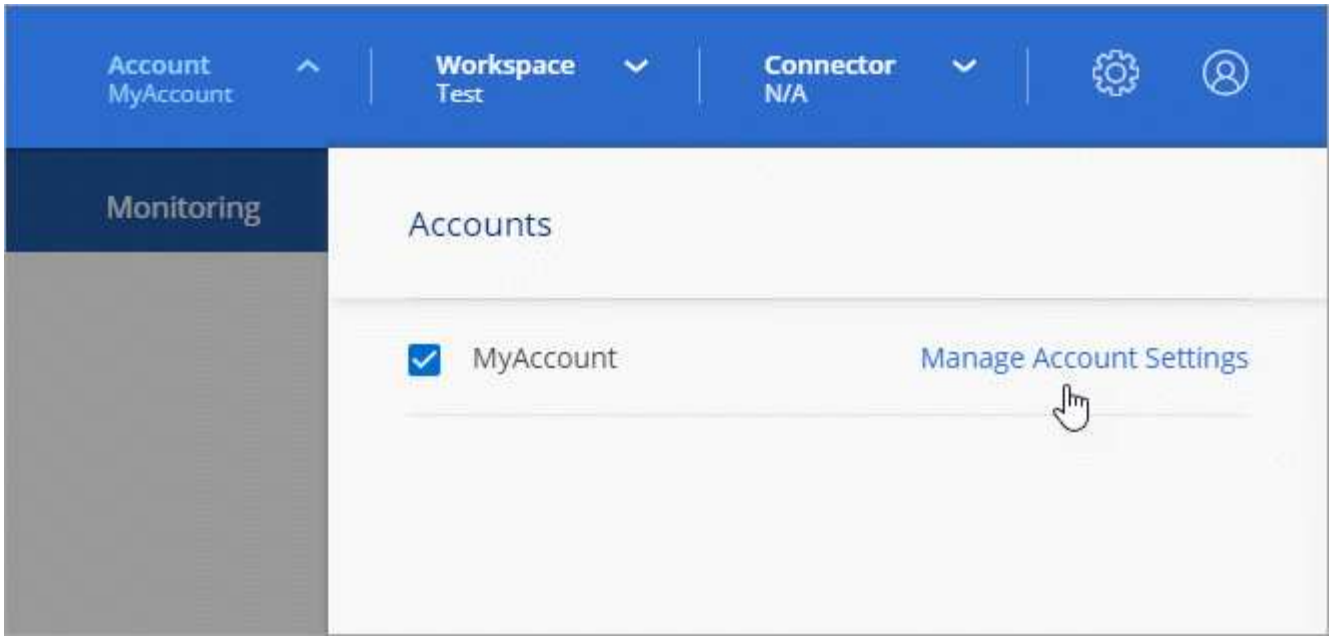
El usuario debe recibir un correo electrónico de Cloud Central de NetApp titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a Cloud Manager.

Quitar usuarios

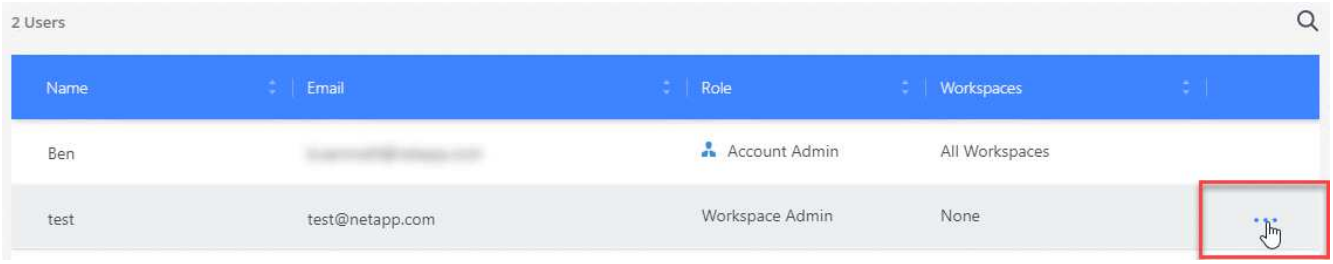
Al desasociar un usuario, éste lo hace para que no pueda acceder a los recursos de una cuenta de Cloud Central.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.



2. En la ficha usuarios , haga clic en el menú acción de la fila correspondiente al usuario.



3. Haga clic en **desasociar usuario** y haga clic en **desasociar** para confirmar.

Resultado

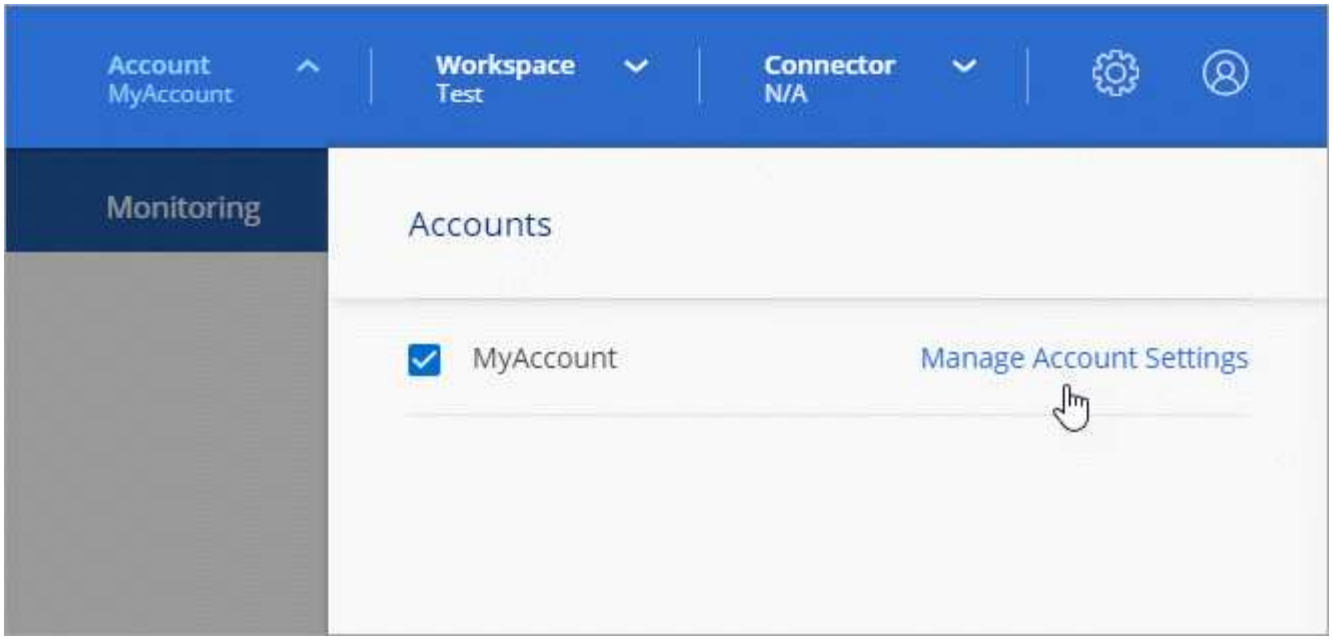
El usuario ya no puede acceder a los recursos de esta cuenta de Cloud Central.

Gestión de los espacios de trabajo de un administrador de área de trabajo

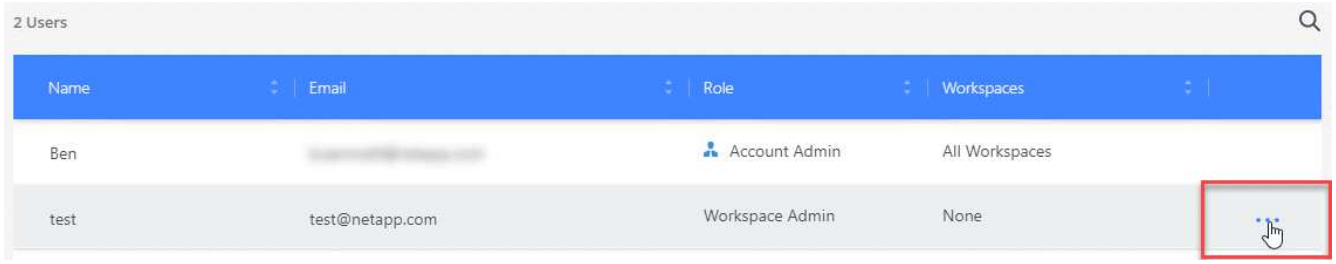
Puede asociar y desasociar administradores de área de trabajo con áreas de trabajo en cualquier momento. La asociación del usuario les permite crear y ver los entornos de trabajo en ese espacio de trabajo.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.



2. En la ficha usuarios , haga clic en el menú acción de la fila correspondiente al usuario.



3. Haga clic en **Administrar espacios de trabajo**.
4. Seleccione los espacios de trabajo que desea asociar con el usuario y haga clic en **aplicar**.

Resultado

Ahora el usuario puede acceder a esos espacios de trabajo desde Cloud Manager, siempre que el conector también esté asociado a los espacios de trabajo.

Gestión de espacios de trabajo

Gestione sus espacios de trabajo creando, cambiando el nombre y borrándolos. Tenga en cuenta que no puede eliminar un área de trabajo si contiene recursos. Debe estar vacío.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. Haga clic en **espacios de trabajo**.
3. Seleccione una de las siguientes opciones:
   - Haga clic en **Agregar nuevo espacio de trabajo** para crear un nuevo espacio de trabajo.
   - Haga clic en **Cambiar nombre** para cambiar el nombre del espacio de trabajo.
   - Haga clic en **Eliminar** para eliminar el área de trabajo.

Gestión de los espacios de trabajo de un conector

Debe asociar el conector a espacios de trabajo para que los administradores de área de trabajo puedan acceder a estos espacios de trabajo desde Cloud Manager.

Si sólo tiene Administradores de cuentas, no es necesario asociar el conector 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, áreas de trabajo y conectores".

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. Haga clic en **conector**.
3. Haga clic en **Administrar áreas de trabajo** para el conector que desea asociar.
4. Seleccione las áreas de trabajo que desea asociar con el conector y haga clic en **aplicar**.

Gestión de suscripciones

Después de suscribirse desde el mercado de un proveedor de cloud, cada suscripción estará disponible en el widget Account Settings. Puede cambiar el nombre de una suscripción y desasociar la suscripción de una o más cuentas.

Por ejemplo, digamos que tiene dos cuentas y cada una se factura mediante suscripciones independientes. Puede desasociar una suscripción de una de las cuentas para que los usuarios de esa cuenta no elijan accidentalmente la suscripción incorrecta al crear un entorno de trabajo de Cloud Volume ONTAP.

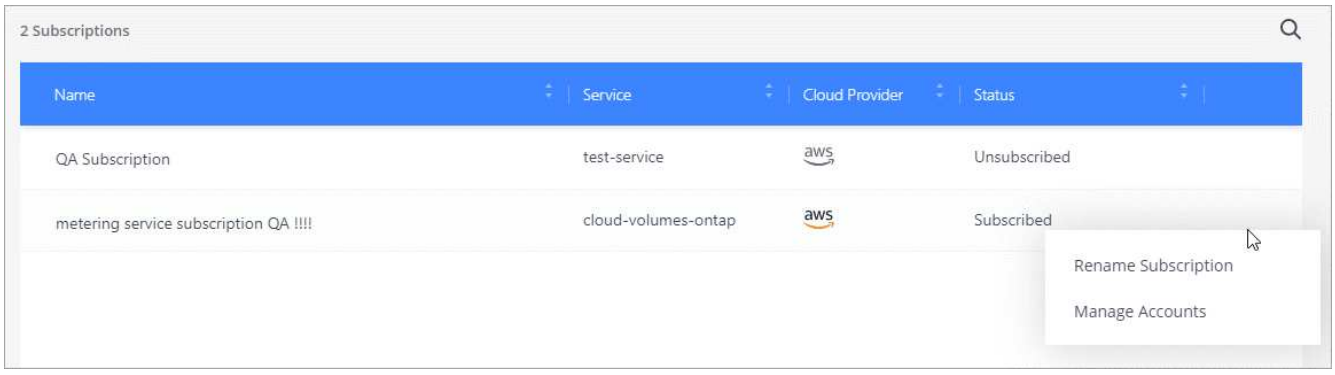
"Más información sobre suscripciones".

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. Haga clic en **Suscripciones**.

   Solo verá las suscripciones asociadas a la cuenta que está viendo actualmente.

3. Haga clic en el menú de acciones de la fila correspondiente a la suscripción que desea administrar.



4. Elija cambiar el nombre de la suscripción o administrar las cuentas asociadas a la suscripción.

Cambiando el nombre de la cuenta

Cambie el nombre de su cuenta en cualquier momento para cambiarlo a algo significativo para usted.

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. En la ficha **Descripción general**, haga clic en el icono de edición situado junto al nombre de la cuenta.
3. Escriba un nuevo nombre de cuenta y haga clic en **Guardar**.

Activación o desactivación de la plataforma SaaS

No recomendamos desactivar la plataforma SaaS a menos que necesite para cumplir con las políticas de seguridad de su empresa. Al deshabilitar la plataforma SaaS, se limita su capacidad para usar los servicios de cloud integrados de NetApp.

Los siguientes servicios no están disponibles en Cloud Manager si deshabilita la plataforma SaaS:

- Cumplimiento de normativas en el cloud
- Kubernetes
- Organización en niveles del cloud
- Caché de archivos global
- Supervisión (Cloud Insights)

Pasos

1. En la parte superior de Cloud Manager, haga clic en el menú desplegable **cuenta** y haga clic en **gestionar cuenta**.
2. En la ficha **Descripción general**, seleccione la opción para activar el uso de la plataforma SaaS.

Gestión de un certificado HTTPS para un 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.

Antes de empezar

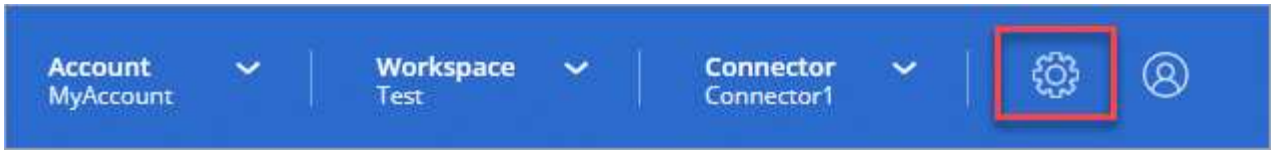
Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Instalar un certificado HTTPS

Instale un certificado firmado por una CA para obtener acceso seguro.

Pasos

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

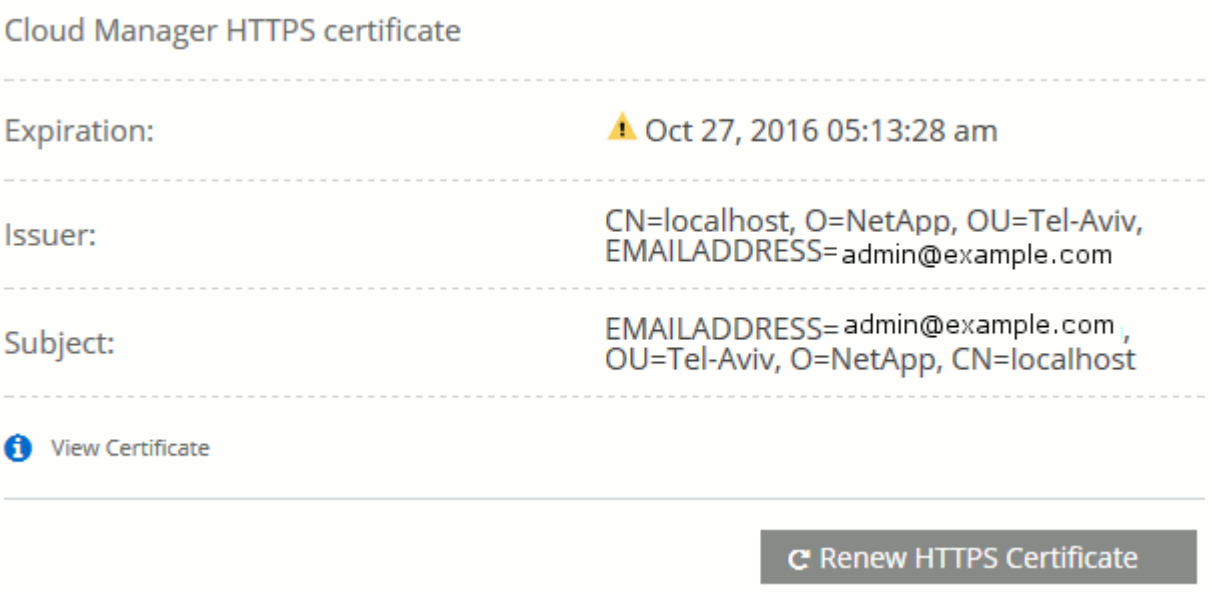


2. En la página HTTPS Setup, instale un certificado generando una solicitud de firma de certificación (CSR) o instalando su propio certificado firmado por una CA:

Opción	Descripción
Genere una CSR	a. Introduzca el nombre de host o DNS del host del conector (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:



Renovando el certificado HTTPS de Cloud Manager

Debe renovar el certificado HTTPS de Cloud Manager antes de que caduque para garantizar el acceso seguro a la consola web de Cloud Manager. Si no renueva el certificado antes de que caduque, aparece una advertencia cuando los usuarios acceden a la consola Web mediante HTTPS.

Pasos

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

   Se muestran detalles sobre el certificado de Cloud Manager, incluida la fecha de vencimiento.

2. Haga clic en **renovar certificado HTTPS** y siga los pasos para generar una CSR o instalar su propio certificado firmado por CA.

Resultado

Cloud Manager usa el nuevo certificado firmado por la CA para proporcionar acceso HTTPS seguro.

Eliminación de entornos de trabajo de Cloud Volumes ONTAP

El administrador de cuentas puede eliminar un entorno de trabajo de Cloud Volumes ONTAP para moverlo a otro sistema o solucionar problemas de detección.

Acerca de esta tarea

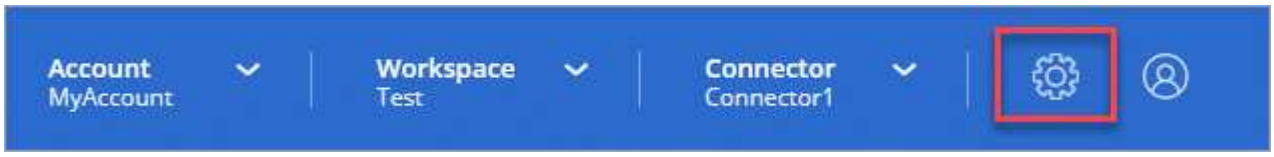
Quitar un entorno de trabajo de Cloud Volumes ONTAP lo elimina de Cloud Manager. No elimina el sistema Cloud Volumes ONTAP. Más tarde podrá volver a descubrir el entorno de trabajo.

La eliminación de un entorno de trabajo de Cloud Manager le permite hacer lo siguiente:

- Redescubrirlo en otro espacio de trabajo
- Redescúbralo en otro sistema Cloud Manager
- Redescubra si tuvo problemas durante el descubrimiento inicial

Pasos

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



2. En la página Herramientas, haga clic en **Iniciar**.
3. Seleccione el entorno de trabajo Cloud Volumes ONTAP que desea quitar.
4. En la página revisar y aprobar, haga clic en **Ir**.

Resultado

Cloud Manager elimina el entorno de trabajo. Los usuarios pueden volver a descubrir este entorno de trabajo desde la página entornos de trabajo en cualquier momento.

Configuración de un conector para utilizar un servidor proxy

Si las directivas de la empresa dictan que utiliza un servidor proxy para todas las comunicaciones HTTP a Internet, debe configurar los conectores para que utilicen ese servidor proxy. El servidor proxy puede estar en la nube o en la red.

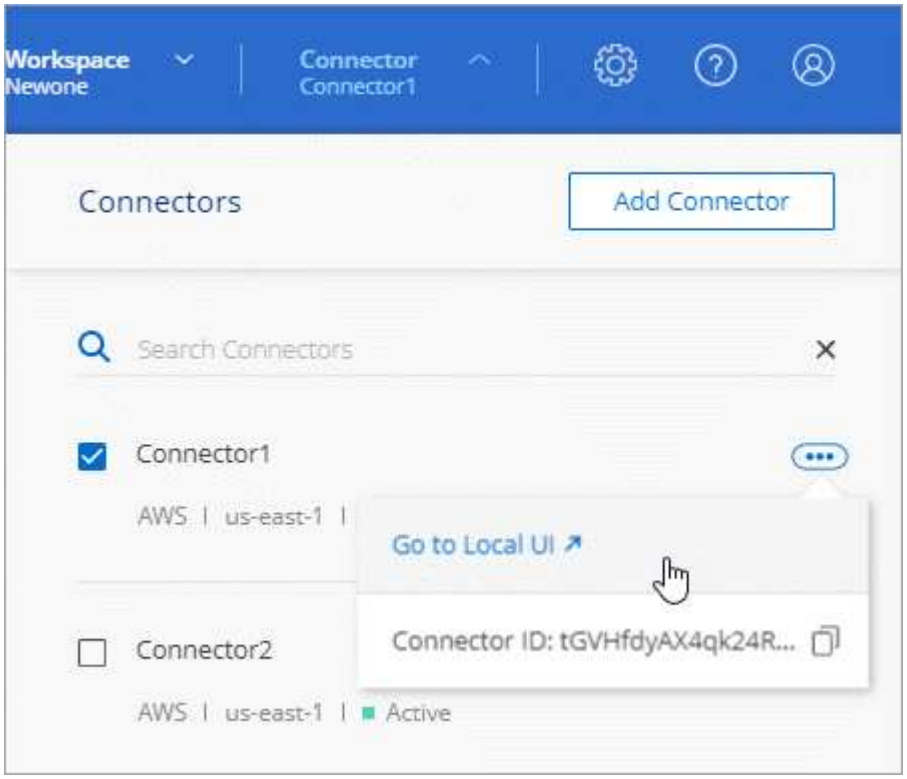
Cuando configura un conector para utilizar un servidor proxy, ese conector y los sistemas Cloud Volumes ONTAP que administra (incluidos los mediadores ha), todos utilizan el servidor proxy.

Pasos

1. "Inicie sesión en la interfaz del SaaS de Cloud Manager" Desde un equipo que tiene una conexión de red a la instancia de conector.

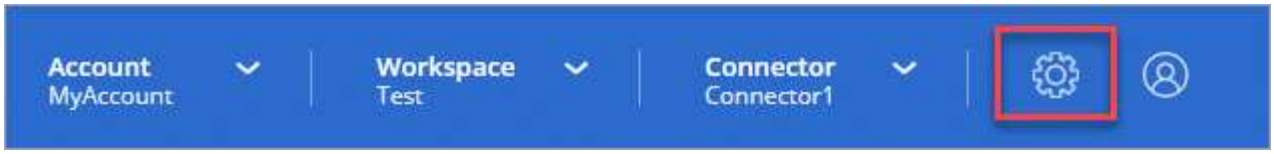
   Si el conector no tiene una dirección IP pública, necesitará una conexión VPN o deberá conectarse desde un host de salto que esté en la misma red que el conector.

2. Haga clic en el menú desplegable **conector** y, a continuación, haga clic en **Ir a la interfaz de usuario local** para ver un conector específico.



   La interfaz de Cloud Manager que se ejecuta en el conector se carga en una nueva pestaña del navegador.

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



4. En HTTP Proxy, introduzca el servidor con la sintaxis http://address:port, especifique un nombre de usuario y una contraseña si se requiere autenticación básica para el servidor y, a continuación, haga clic en Guardar.

Cloud Manager no admite contraseñas con el carácter @.

Resultado

Después de especificar el servidor proxy, los nuevos sistemas Cloud Volumes ONTAP se configuran automáticamente para utilizar el servidor proxy al enviar mensajes de AutoSupport. Si no especificó el servidor proxy antes de que los usuarios crearan sistemas Cloud Volumes ONTAP, deben usar System Manager para establecer manualmente el servidor proxy en las opciones de AutoSupport para cada sistema.

Anulación de los bloqueos de CIFS para la alta disponibilidad de Cloud Volumes ONTAP en Azure

El administrador de cuentas puede habilitar un ajuste en Cloud Manager para evitar problemas con la conmutación por error del almacenamiento de Cloud Volumes ONTAP durante eventos de mantenimiento de Azure. Cuando se habilita este ajuste, Cloud Volumes ONTAP veta CIFS locks y restablece las sesiones CIFS activas.

Acerca de esta tarea

Microsoft Azure programa eventos de mantenimiento periódicos en sus máquinas virtuales. Cuando se produce un evento de mantenimiento en un nodo de un par de alta disponibilidad de Cloud Volumes ONTAP, el par de alta disponibilidad inicia la toma de control del almacenamiento. Si hay sesiones CIFS activas durante este evento de mantenimiento, los bloqueos de archivos CIFS pueden evitar la conmutación por error del almacenamiento.

Si se habilita esta configuración, Cloud Volumes ONTAP vetará los bloqueos y restablecerá las sesiones CIFS activas. Como resultado, la pareja de alta disponibilidad puede completar los procesos de conmutación por error del almacenamiento durante estos eventos de mantenimiento.

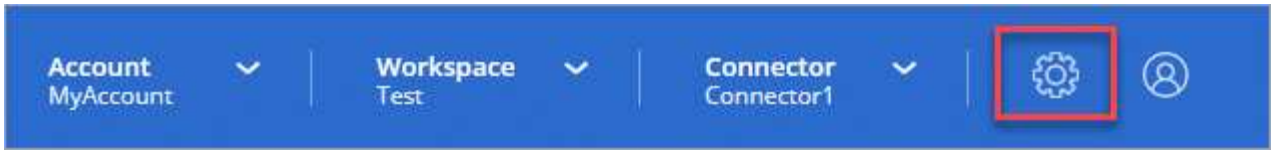
Este proceso puede provocar interrupciones en los clientes CIFS. Se pueden perder los datos que no están comprometidos con los clientes CIFS.

Lo que necesitará

Debe crear un conector antes de poder cambiar la configuración de Cloud Manager. "Vea cómo".

Pasos

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



2. En **bloqueos CIFS ha**, seleccione la casilla de verificación y haga clic en **Guardar**.

Referencia

Funciones

Las funciones Administrador de cuentas, Administrador de área de trabajo y Visor de cumplimiento de la nube proporcionan permisos específicos a los usuarios.

Tarea	Administrador de cuentas	Administrador de área de trabajo	Visor de cumplimiento de normativas cloud
Gestionar entornos de trabajo	Sí	Sí	No
Activar servicios en entornos de trabajo	Sí	Sí	No
Ver el estado de replicación de datos	Sí	Sí	No
Visualice la línea de tiempo	Sí	Sí	No
Cambiar entre espacios de trabajo	Sí	Sí	Sí
Ver resultados de análisis de cumplimiento	Sí	Sí	Sí
Eliminar entornos de trabajo	Sí	No	No
Conecte los clústeres de Kubernetes a entornos de trabajo	Sí	No	No
Reciba el informe de Cloud Volumes ONTAP	Sí	No	No
Crear conectores	Sí	No	No
Administrar cuentas de Cloud Central	Sí	No	No
Gestionar credenciales	Sí	No	No
Modifique la configuración de Cloud Manager	Sí	No	No
Consulte y gestione la consola de soporte	Sí	No	No
Elimine entornos de trabajo de Cloud Manager	Sí	No	No
Instale un certificado HTTPS	Sí	No	No

Enlaces relacionados

- "Configuración de espacios de trabajo y usuarios en la cuenta de Cloud Central"
- "Gestión de espacios de trabajo y usuarios en la cuenta de Cloud Central"

Cómo Cloud Manager utiliza los permisos de proveedores de cloud

Cloud Manager requiere permisos para realizar acciones en su proveedor de cloud. Estos permisos se incluyen en "Las políticas proporcionadas por NetApp". Tal vez desee entender qué hace Cloud Manager con estos permisos.

Qué hace Cloud Manager con los permisos de AWS

Cloud Manager utiliza una cuenta de AWS para realizar llamadas API a varios servicios de AWS, incluidos EC2, S3, CloudFormation, IAM, Security Token Service (STS) y el servicio de gestión de claves (KMS).

Acciones	Específico
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeInstances", "ec2:DescribeInstanceStatus", "ec2:RunInstances", "ec2:TerminateInstances", "ec2:ModificyAttribute",	Inicia una instancia de Cloud Volumes ONTAP y detiene, inicia y supervisa la instancia.
"ec2:DescribeInstanceAttribute",	Verifica que las redes mejoradas están habilitadas para los tipos de instancia admitidos.
"ec2:DescribeRouteTables", "ec2:DescribeImages",	Inicia una configuración de alta disponibilidad de Cloud Volumes ONTAP.
"ec2:CreateTags",	Etiqueta todos los recursos que Cloud Manager crea con las etiquetas "WorkingEnvironment" y "WorkingEnvironmentId". Cloud Manager utiliza estas etiquetas para tareas de mantenimiento y asignación de costes.
"ec2:CreateVolume", "ec2:DescribeVolumes", "ec2:ModifyVolumeAttribute", "ec2:AttachVolume", "ec2:DeleteVolume", "ec2:DetachVolume",	Gestiona los volúmenes de EBS que Cloud Volumes ONTAP utiliza como almacenamiento back-end.
"ec2:CreateSecurityGroup", "ec2:DeleteSecurityGroup", "ec2:DescribeSecurityGroups", "ec2:RevokeSecurityGroupEgress", "ec2:AuthorizeSecurityGroupEgress", "ec2:AuthorizeGroupSecurityGroupIngress", "ec2:RevokeSecurityGroupIngress",	Crea grupos de seguridad predefinidos para Cloud Volumes ONTAP.
"ec2:CreateNetworkInterface", "ec2:DescribeNetworkInterface", "ec2:DeleteNetworkInterface", "ec2:ModifyNetworkInterfaceAttribute",	Crea y administra interfaces de red para Cloud Volumes ONTAP en la subred de destino.
"ec2:DescribeSubnets", "ec2:DescribeVpcs",	Obtiene la lista de subredes de destino y grupos de seguridad, que se necesita al crear un nuevo entorno de trabajo para Cloud Volumes ONTAP.

Acciones	Específico
"ec2:DescribDhcpOptions",	Determina los servidores DNS y el nombre de dominio predeterminado al iniciar instancias de Cloud Volumes ONTAP.
"ec2:CreateSnapshot", "ec2:DeleteSnapshot", "ec2:DescribeSnapshots",	Toma snapshots de volúmenes de EBS durante la configuración inicial y cada vez que se detiene una instancia de Cloud Volumes ONTAP.
"ec2:GetConsoleOutput",	Captura la consola de Cloud Volumes ONTAP, que está conectada a mensajes de AutoSupport.
"ec2:DescribeKeyPairs",	Obtiene la lista de pares de claves disponibles al iniciar instancias.
"ec2:regiones describidas",	Obtiene una lista de las regiones disponibles de AWS.
"ec2:DeleteTags", "ec2:DescribeTags",	Gestiona etiquetas de los recursos asociados a instancias de Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:Describestacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Inicia instancias de Cloud Volumes ONTAP.
"iam:PassRole", "iam:CreateRole", "iam:DeleteRole", "iam:PutRolePolicy", "iam:CreateInstanceProfile", "iam:DeleteRololePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "DeleteInstanceProfile"	Inicia una configuración de alta disponibilidad de Cloud Volumes ONTAP.
"iam:ListInstanceProfiles", "sts:DecodeAuthorizationMessage", "ec2:AssociateIamInstanceProfile", "ec2:DescribeIamInstanceProfileAssociations", "ec2:DisasociateIamanceProfile",	Administra perfiles de instancia para instancias de Cloud Volumes ONTAP.
"s3:GetBucketTagging", "s3:GetBucketLocation", "s3:ListAllMyBuckets", "s3:ListBucket"	Obtiene información sobre cubos de AWS S3 para que Cloud Manager pueda integrarse con el servicio Data Fabric Cloud Sync de NetApp.
"s3:CreateBucket", "s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutBucketTagging", "s3:ListBucketVersions", "bucs3:GetBucketPolicyStatus", "s3:GetBucketAccessBlock", "PublicGetS3:GetPutketPolicy", "buckets3", "buckets3:AccessPolicy"	Gestiona el bloque de S3 que un sistema Cloud Volumes ONTAP utiliza como nivel de capacidad para la organización de datos en niveles.
"Kms:List*", "kms:Recifrar*", "kms:describir*", "kms:CreateGrant",	Habilita el cifrado de datos de Cloud Volumes ONTAP mediante el Servicio de gestión de claves (KMS) de AWS.

Acciones	Específico
"ce:GetReservationUtilization", "CE:GetDimensionValues", "CE:GetCostAndUsage", "CE:getTags"	Obtiene los datos de costes de AWS para Cloud Volumes ONTAP.
"ec2:CreatePlacementGroup", "ec2:DeletePlacementGroup"	Al poner en marcha una configuración de alta disponibilidad en una única zona de disponibilidad de AWS, Cloud Manager lanza los dos nodos de alta disponibilidad y el mediador en un grupo de colocación extendido de AWS.
"ec2:DescribeReservedInstancesOfferings"	Cloud Manager utiliza el permiso como parte de la implementación de Cloud Compliance para elegir el tipo de instancia que desea utilizar.
"s3:DeleteBucket", "s3:GetLifecycleConfiguration", "s3:PutLifecycleConfiguration", "s3:PutketPolicyTaging", "s3:ListBucketVersions", "s3:BucketBucketBucket", "s3:ListAccessAllAccessMyBuckets", "s3:GetBucketPolicyPolicy", "getbuckets3", "BucketS3:GetBucketBucketBucketBucketBlock", "BucketS3", "BucketS3:GetBucketS3", "BucketBucketS3", "GetBucketBucketBucketBucketBucketBucketBucketBucketBucketBlock",", "	Cloud Manager utiliza estos permisos cuando se habilita el servicio Backup en S3.

Qué hace Cloud Manager con permisos de Azure

La política de Cloud Manager para Azure incluye los permisos que necesita Cloud Manager para implementar y gestionar Cloud Volumes ONTAP en Azure.

Acciones	Específico
"Microsoft.Compute/locations/operations/read", "Microsoft.Compute/locations/vmSizes/read", "Microsoft.Compute/operations/read", "Microsoft.Compute/virtualMachines/instanceView/read", "Microsoft.Compute/virtualMachines/powerOff/action", "Microsoft.Compute/virtualMachines/read", "Microsoft.Compute/virtualMachines/restart/action", "Microsoft.Compute/virtualMachines/start/action", "Microsoft.Compute/virtualMachines/deallocate/action", "Microsoft.Compute/virtualMachines/vmSizes/read", "Microsoft.Compute/virtualMachines/write",	Crea Cloud Volumes ONTAP y detiene, inicia, elimina y obtiene el estado del sistema.
"Microsoft.Compute/images/write", "Microsoft.Compute/images/read",	Permite la puesta en marcha de Cloud Volumes ONTAP desde un disco duro virtual.

Acciones	Específico
"Microsoft.Compute/disks/delete", "Microsoft.Compute/disks/read", "Microsoft.Compute/disks/write", "Microsoft.Storage/checknameAvailability/read", "Microsoft.Storage/opers/read", "Microsoft.Storage/storageAccounts/listkeys/action", "Microsoft.Storage/Accounts/read", "Microsoft.Storage/storageAccounts/regeneratekey/action", "Microsoft.Storage/Storage Accounts/write", "Storage.files/Storage/Storage/Storage Accounts", "	Gestiona cuentas de almacenamiento y discos de Azure y conecta los discos a Cloud Volumes ONTAP.
"Microsoft.Network/networkInterfaces/read", "Microsoft.Network/networkInterfaces/write", "Microsoft.Network/networkInterfaces/join/action",	Crea y administra interfaces de red para Cloud Volumes ONTAP en la subred de destino.
"Microsoft.Network/networkSecurityGroups/read", "Microsoft.Network/networkSecurityGroups/write", "Microsoft.Network/networkSecurityGroups/join/action",	Crea grupos de seguridad de red predefinidos para Cloud Volumes ONTAP.
"Microsoft.Resources/subscripciones/ubicaciones/lecturas", "Microsoft.Network/locations/operationResults/read", "Microsoft.Network/locations/operations/read", "Microsoft.Network/virtualNetworks/read", "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", "Microsoft.Network/virtualNetworks/subnets/read", "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", "Microsoft.Network/virtualNetworks/virtualMachines/read", "Microsoft.Network/virtualNetworks/subnets/join/action",	Obtiene información de red acerca de las regiones, la red virtual de destino y la subred, y agrega Cloud Volumes ONTAP a las redes virtuales.
"Microsoft.Network/virtualNetworks/subnets/write", "Microsoft.Network/routeTables/join/action",	Habilita extremos de servicio vnet para organizar los datos en niveles.
"Microsoft.Resources/despliegues/operaciones/lectura", "Microsoft.Resources/despliegues/read", "Microsoft.Resources/despliegues/write",	Implementa Cloud Volumes ONTAP a partir de una plantilla.

Acciones	Específico
"Microsoft.Resources/despliegues/operacions/read", "Microsoft.Resources/despliegues/read", "Microsoft.Resources/despliegues/write", "Microsoft.Resources/resources/read", "Microsoft.Resources/Resources/operationResults/read", "Microsoft.Resources/subscripciones/ResourceGroups/delete", "Microsoft.Resources/subscripciones/Groups/read/resources", "ResourceGroups/subscripciones"/resources/Microsoft.Resources/subscriptions/Microsoft","/resources/subscripciones"/resources/Microsoft.Microsoft/resources/resources/Microsoft.read/subscriptions/resources	Crea y gestiona grupos de recursos para Cloud Volumes ONTAP.
"Microsoft.Compute/snapshots/write", "Microsoft.Compute/snapshots/read", "Microsoft.Compute/disks/beginGetAccess/action"	Crea y gestiona copias Snapshot gestionadas de Azure.
"Microsoft.Compute/availabilitySets/write", "Microsoft.Compute/availabilitySets/read",	Crea y administra conjuntos de disponibilidad para Cloud Volumes ONTAP.
"Microsoft.MarketPlaceorders/offertypes/editoriales/Ofertas/planes/acuerdos/leídos", "Microsoft.MarketPlaceoring/offertypes/editoriales/Ofertas/planes/acuerdos/escribir"	Permite puestas en marcha mediante programación desde Azure Marketplace.
"Microsoft.Network/loadBalancers/read", "Microsoft.Network/loadBalancers/write", "Microsoft.Network/loadBalancers/delete", "Microsoft.Network/loadBalancers/backendAddressPools/read", "Microsoft.Network/loadBalancers/backendAddressPools/join/action", "Microsoft.Network/loadBalancers/frontendIPConfigurations/read", "Microsoft.Network/loadBalancers/loadBalancingRules/read", "Microsoft.Network/loadBalancers/probes/read", "Microsoft.Network/loadBalancers/probes/join/action",	Gestiona un equilibrador de carga de Azure para pares de alta disponibilidad.
"Microsoft.Autorizaciones/bloqueos/*"	Permite la gestión de bloqueos en discos de Azure.
"Microsoft.Authorization/roleDefinitions/write", "Microsoft.Authorization/roleAssignments/write", "Microsoft.Web/sites/*"	Gestiona la conmutación por error para pares de alta disponibilidad.

Acciones	Específico
"Microsoft.Network/privateEndpoints/write", "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action", "Microsoft.Storage/storageAccounts/privateEndpointConnections/read", "Microsoft.Network/privateEndpoints/read", "Microsoft.Network/privateDnsZones/write", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", "Microsoft.Network/virtualNetworks/join/action", "Microsoft.Network/privateDnsZones/A/write", "Microsoft.Network/privateDnsZones/read", "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",	Permite la gestión de extremos privados. Los extremos privados se utilizan cuando no se proporciona conectividad fuera de la subred. Cloud Manager crea la cuenta de almacenamiento para alta disponibilidad con solo conectividad interna en la subred.
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Permite a Cloud Manager eliminar volúmenes para Azure NetApp Files.
"Microsoft.Resources/despliegues/operationStatuses/Read"	Azure requiere este permiso para algunas implementaciones de máquinas virtuales (depende del hardware físico subyacente que se haya utilizado durante la implementación).
"Microsoft.Resources/despliegues/operationStatuses/read", "Microsoft.Insights/Metrics/Read", "Microsoft.Compute/virtualMachines/extensions/write", "Microsoft.Compute/virtualMachines/extensions/read", "Microsoft.Compute/virtualMachines/extensions/delete", "Microsoft.Compute/virtualMachines/delete", "Microsoft.Network/networkInterfaces/delete", "Microsoft.Network/networkSecurityGroups/delete", "Microsoft.Resources/despliegues/delete",	Permite usar la caché de archivos global.
"Microsoft.Compute/diskEncryptionSets/read"	Permite a Cloud Manager cifrar discos gestionados de Azure en sistemas Cloud Volumes ONTAP de un solo nodo mediante claves externas de otra cuenta. Esta función es compatible con el uso de API.

Qué hace Cloud Manager con los permisos de GCP

La política de Cloud Manager para GCP incluye los permisos que Cloud Manager necesita para implementar y gestionar Cloud Volumes ONTAP.

Acciones	Específico
- Compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Para crear y gestionar discos para Cloud Volumes ONTAP.
- computar.firewalls.create - compute.firewalls.delete - computar.firewalls.get - computar.firewalls.list	Para crear reglas de firewall para Cloud Volumes ONTAP.
- Compute.globalOperations.get	Para obtener el estado de las operaciones.

Acciones	Específico
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Para obtener imágenes para instancias de equipos virtuales.
- compute.instances.attachDisk - compute.instances.detachDisk	Para conectar y desconectar discos en Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Para crear y eliminar instancias de Cloud Volumes ONTAP VM.
- compute.instances.get	Para mostrar instancias de máquina virtual.
- compute.instances.getSerialPortOutput	Para obtener los registros de la consola.
- compute.instances.list	Para recuperar la lista de instancias de una zona.
- compute.instances.setDeletionProtection	Para establecer la protección de eliminación en la instancia.
- compute.instances.setLabels	Para agregar etiquetas.
- compute.instances.setMachineType	Para cambiar el tipo de máquina para Cloud Volumes ONTAP.
- compute.instances.setMetadata	Para añadir metadatos.
- compute.instances.setTags	Para agregar etiquetas para reglas de firewall.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Para iniciar y detener Cloud Volumes ONTAP.
- computar.machineTypes.get	Para obtener el número de núcleos para comprobar qoutras.
- compute.projects.get	Para dar soporte a proyectos múltiples.
- Compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	Para crear y gestionar instantáneas de disco persistentes.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regises.list - compute.subnetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.list	Para obtener la información de red necesaria para crear una nueva instancia de máquina virtual de Cloud Volumes ONTAP.

Acciones	Específico
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifest.list - deploymentmanager.opers.get - deploymentmanager.opers.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.Types.get - deploymentmanager.types.list	Para poner en marcha la instancia de máquina virtual de Cloud Volumes ONTAP mediante Google Cloud Deployment Manager.
- logEntries.list - logging.privateLogEntries.list	Para obtener unidades de registro de pila.
- resourcemanager.projects.get	Para dar soporte a proyectos múltiples.
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	Para crear y gestionar un bucket de Google Cloud Storage para la organización de datos en niveles.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudKMS.cryptoKeys.get - cloudKMS.cryptoKeys.list - cloudKMS.Keyring.list	Para utilizar claves de cifrado gestionadas por el cliente desde el Servicio de gestión de claves cloud con Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	Para establecer una cuenta de servicio en la instancia de Cloud Volumes ONTAP. Esta cuenta de servicio proporciona permisos para organizar los datos en niveles en un bloque de Google Cloud Storage.

Páginas de AWS Marketplace para Cloud Manager y Cloud Volumes ONTAP

Existen varias ofertas disponibles en el mercado de AWS para Cloud Manager y Cloud Volumes ONTAP. Si necesita ayuda para entender el propósito de cada página, lea las descripciones a continuación.

En todos los casos, recuerde que no puede iniciar Cloud Volumes ONTAP en AWS desde AWS Marketplace. Es necesario iniciar directamente desde Cloud Manager.

Objetivo	Página AWS Marketplace para utilizar	Más información
Habilite el uso de Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance y otros servicios adicionales	"Cloud Manager: Ponga en marcha y gestione los servicios de datos en el cloud de NetApp"	Esta suscripción permite cobrar la versión de PAYGO de Cloud Volumes ONTAP 9.6 y posterior. También permite cobrar los niveles del cloud, Cloud Compliance y otros servicios adicionales. Deberá suscribirse a esta oferta cuando Cloud Manager le solicite y le redireccione a la página. Cloud Manager le solicita en el asistente de entorno de trabajo o cuando agrega nuevas credenciales en Configuración. Esta página no le permite iniciar Cloud Manager en AWS. Eso se debe hacer desde "Cloud Central de NetApp"O bien, utilizando el AMI que se indica en la fila 3 de esta tabla.
Habilite el uso de Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance y otros servicios adicionales *usando un contrato anual*	"Cloud Manager (contratos): Implemente gestione los servicios de datos en el cloud de NetApp"	Esta suscripción es una alternativa a la suscripción en la primera fila. Le permite obtener un pago inicial anual para los listings. En la mayoría de los casos está destinada a partners de NetApp.
Ponga en marcha Cloud Manager desde AWS Marketplace mediante un AMI	"Cloud Manager: Instalación manual sin claves de acceso"	Le recomendamos que ejecute Cloud Manager en AWS desde "Cloud Central de NetApp", pero puede iniciarlo desde esta página de AWS Marketplace, si lo prefiere.
Permitir la puesta en marcha de Cloud Volumes ONTAP PAYGO (9.5 o anterior)	• "Cloud Volumes ONTAP para AWS" • "Cloud Volumes ONTAP para AWS: Alta disponibilidad"	Estas páginas de AWS Marketplace le permiten suscribirse a las versiones de nodo único o ha de Cloud Volumes ONTAP PAYGO para las versiones 9.5 y anteriores. A partir de la versión 9.6, tiene que suscribirse a la página de AWS Marketplace que se encuentra en la fila 1 de esta tabla para las puestas en marcha de PAYGO.