# Gestionar credenciales

## Cloud Manager 3.8

NetApp
March 25, 2024

# Tabla de contenidos

# Gestionar credenciales

# AWS

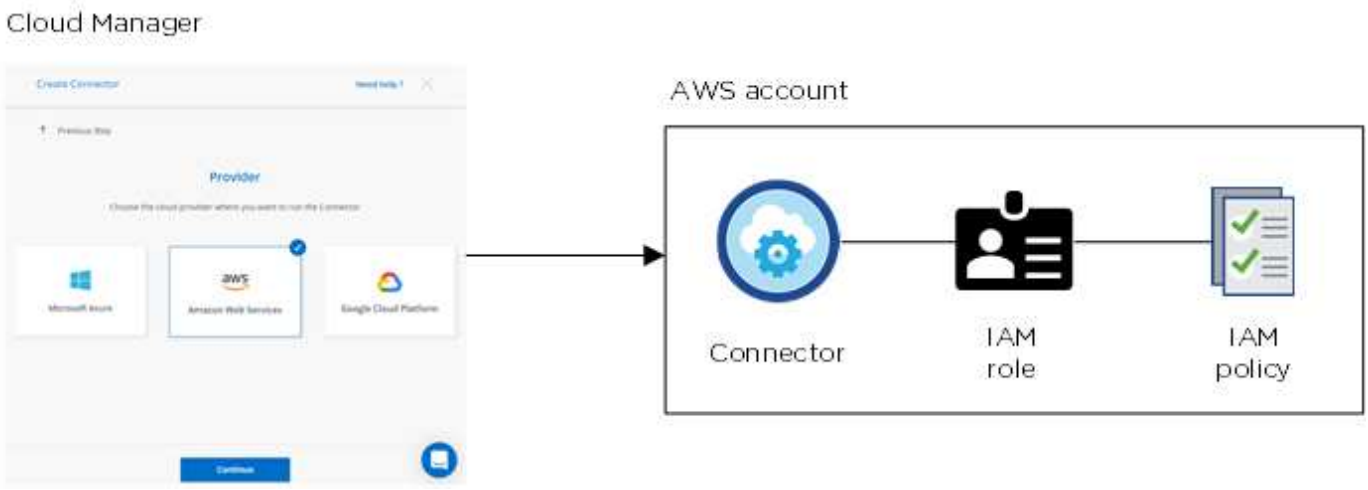
## Credenciales y permisos de AWS

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.

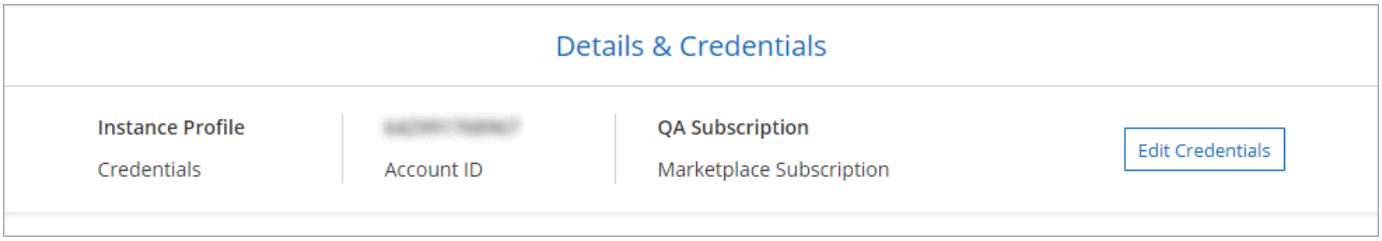
### Credenciales iniciales de AWS

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".



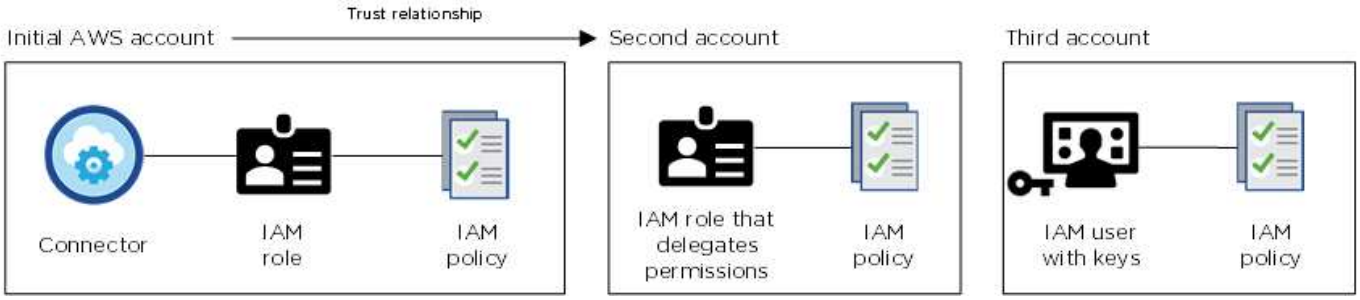

Cloud Manager selecciona estas credenciales de AWS de forma predeterminada al crear un entorno de trabajo nuevo para Cloud Volumes ONTAP:




### Credenciales adicionales de AWS

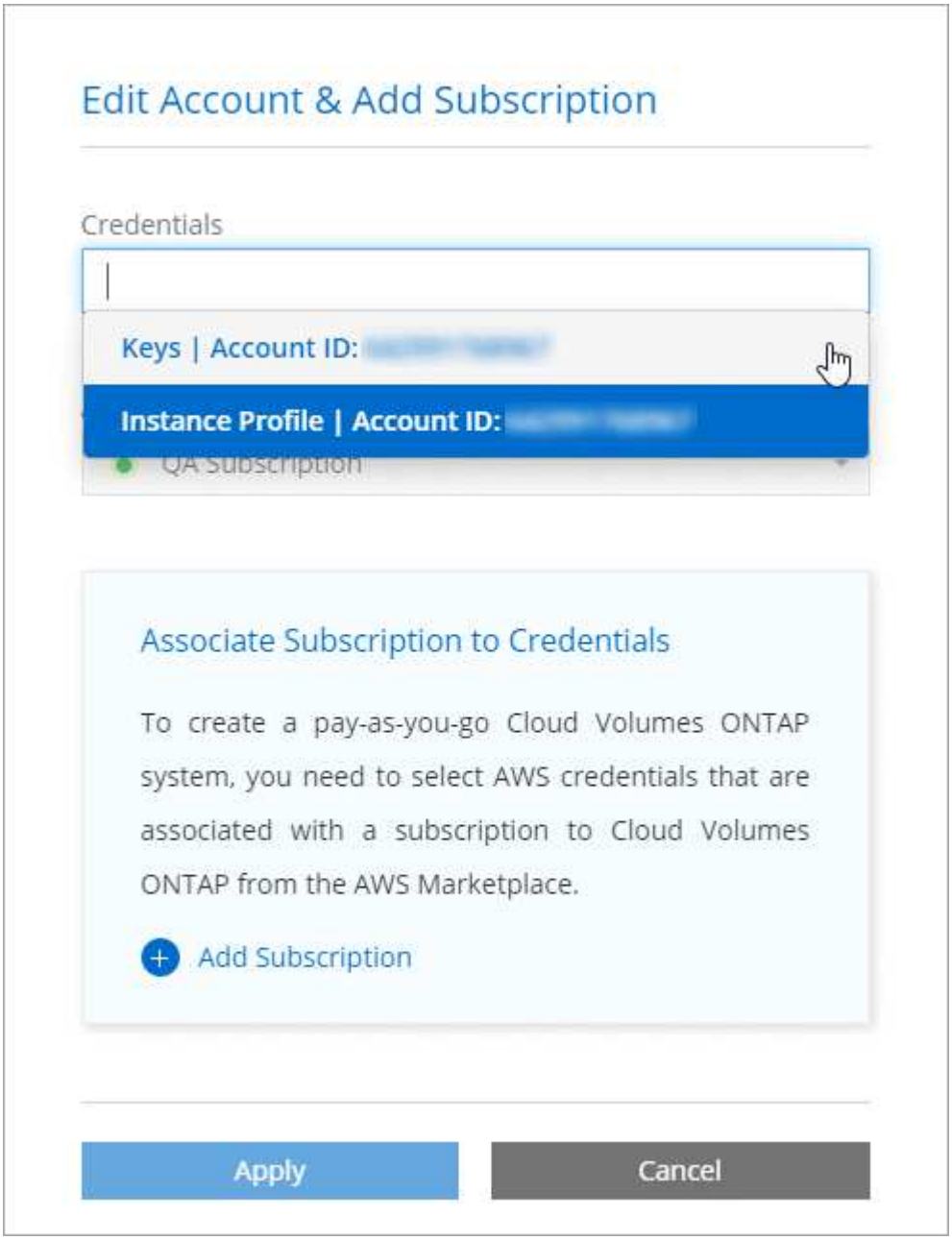
Si desea ejecutar Cloud Volumes ONTAP en diferentes cuentas de AWS, puede hacerlo también "Proporcione las claves AWS para un usuario de IAM o el ARN de un rol en una cuenta de confianza". En la siguiente

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

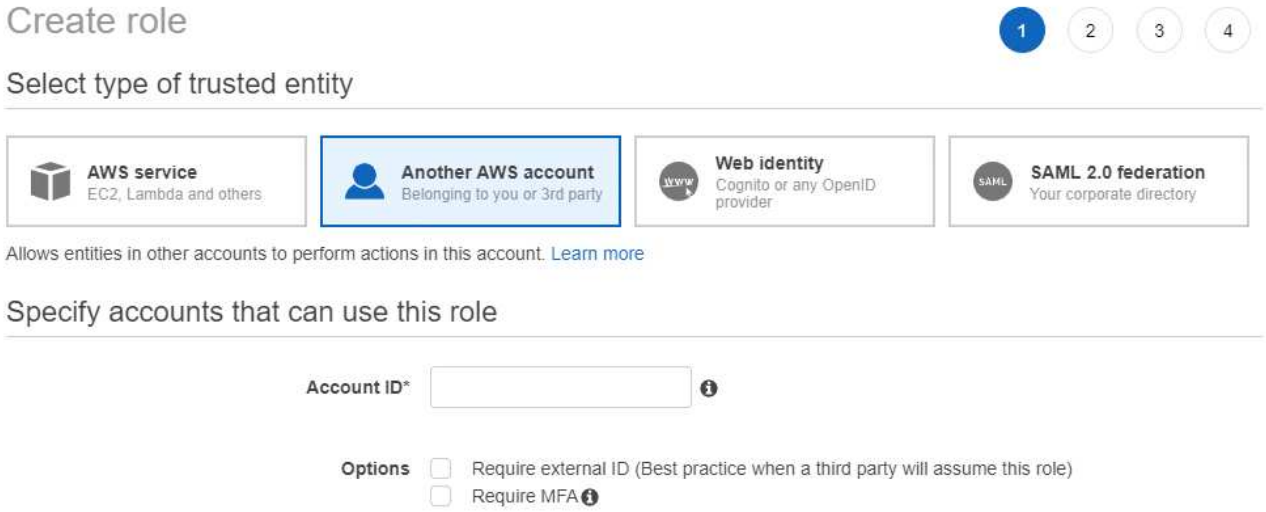
Puede configurar una relación de confianza entre la cuenta AWS de origen en la que ha implementado la instancia de Connector y otras cuentas de AWS mediante los roles IAM. A continuación, debe proporcionar a Cloud Manager el ARN de las funciones de IAM de las cuentas de confianza.

**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**

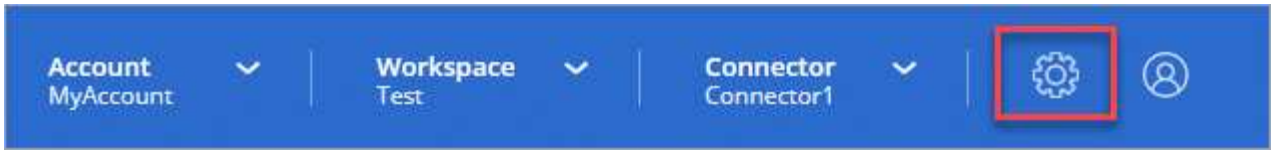
La cuenta ahora tiene los permisos necesarios. Ahora puede añadirlo a Cloud Manager.

### 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**.



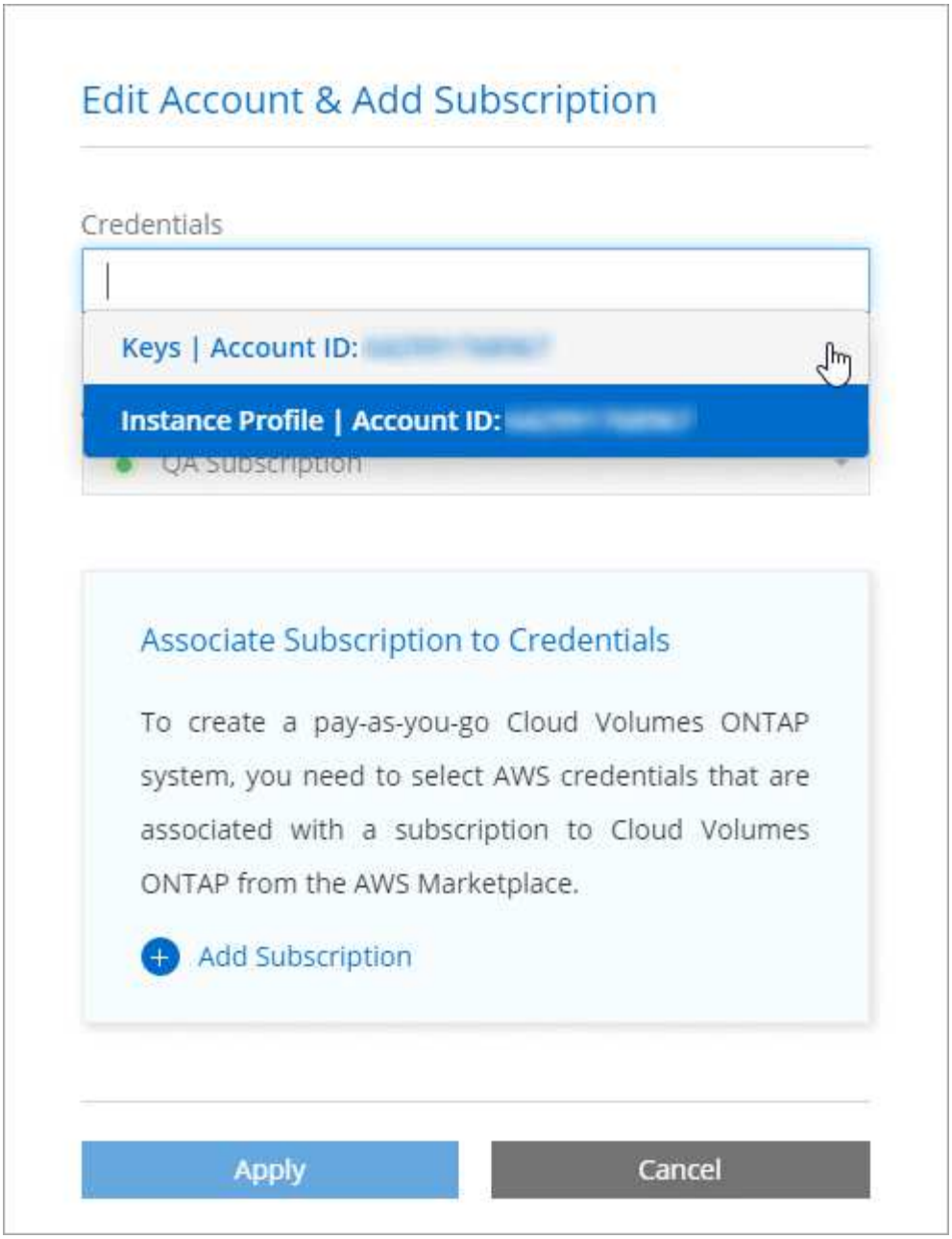

2. Haga clic en **Agregar credenciales** y seleccione **AWS**.
3. Proporcione las claves AWS o el ARN del rol de IAM de confianza.
4. Confirme que se han cumplido los requisitos de la directiva y haga clic en **continuar**.
5. Elija la suscripción de pago por uso que desee asociar con las credenciales 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:

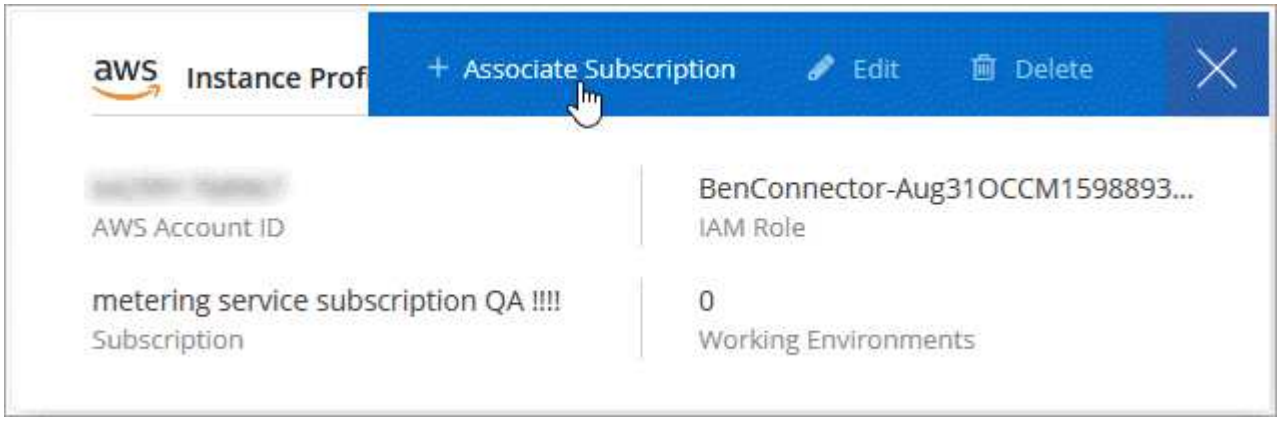
- No asoció una suscripción al agregar inicialmente las credenciales a Cloud Manager.
- Desea sustituir una suscripción existente de AWS Marketplace por una nueva suscripción.

**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

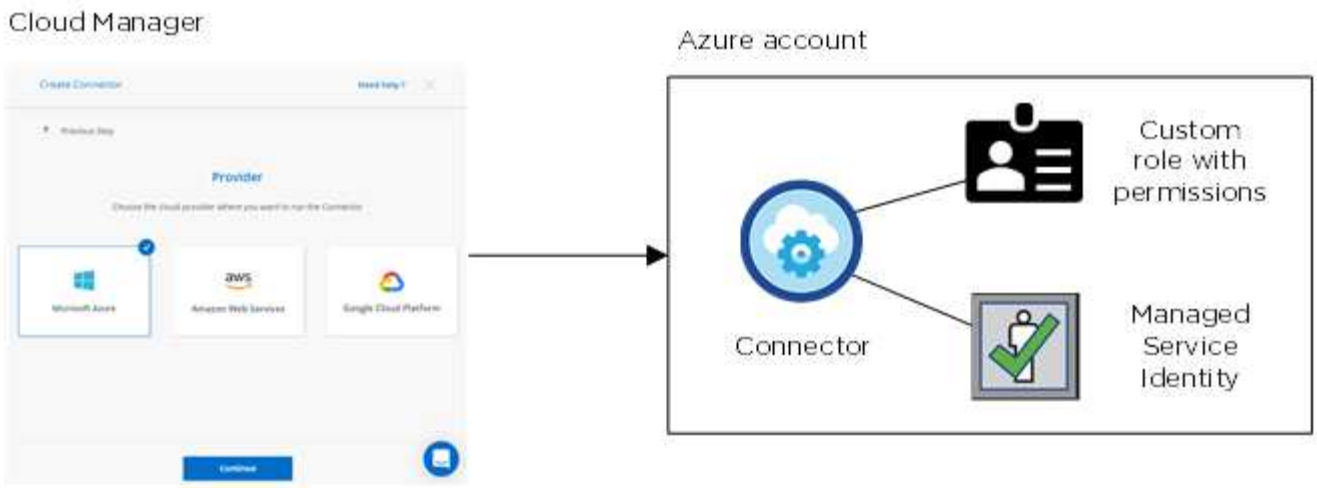
## Credenciales y permisos de Azure

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.

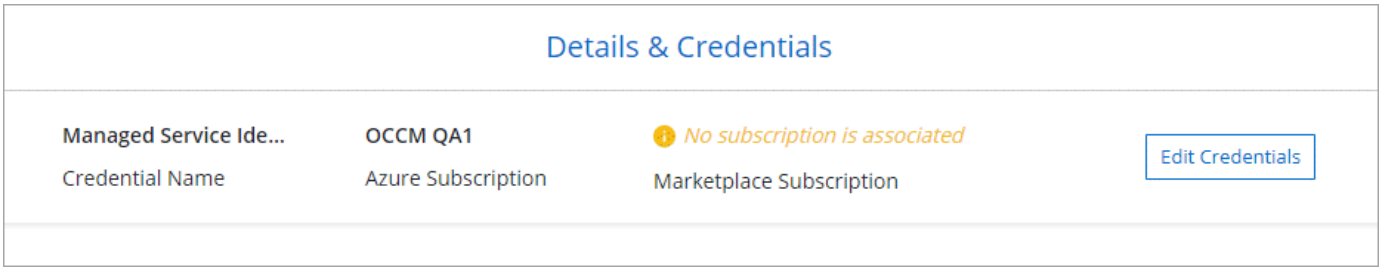
### Credenciales iniciales de Azure

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:

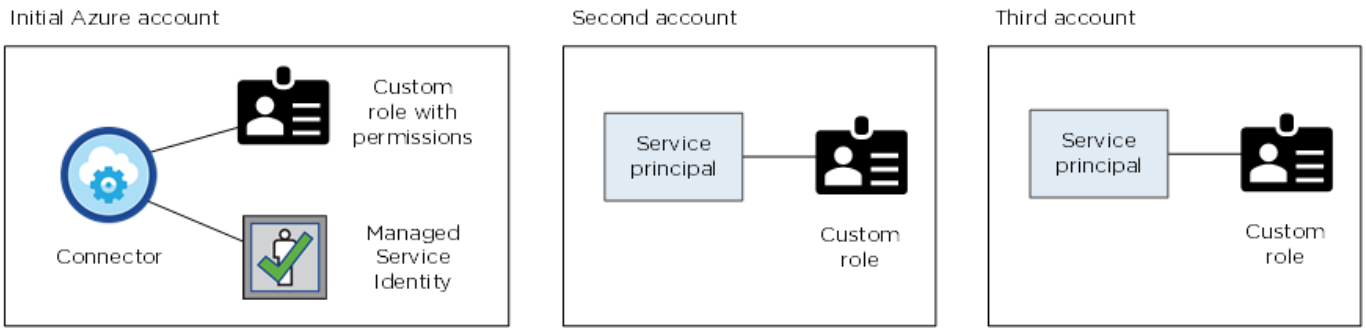



### Suscripciones adicionales de Azure para una identidad gestionada

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".

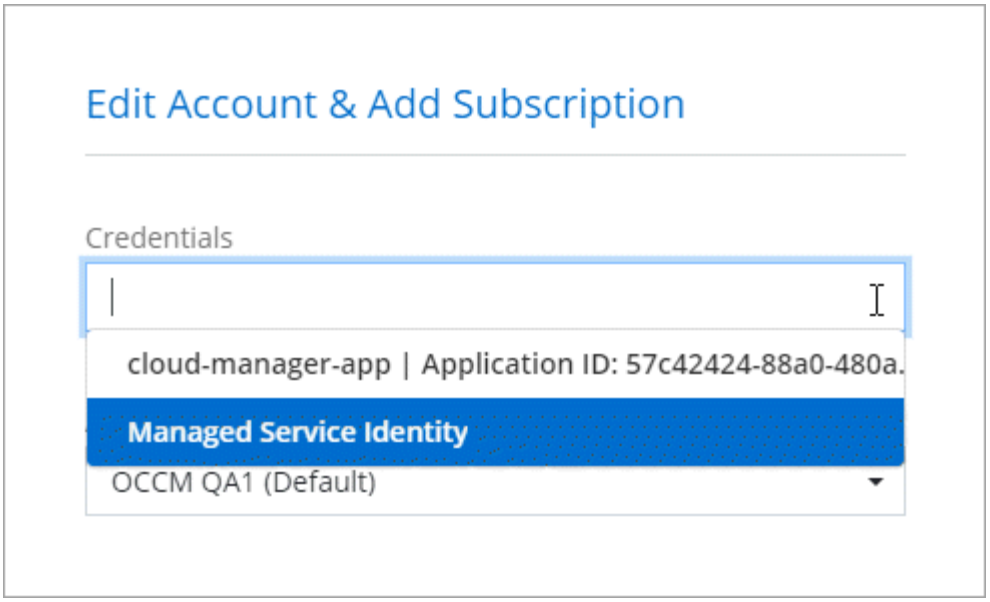
### Credenciales adicionales de Azure

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.

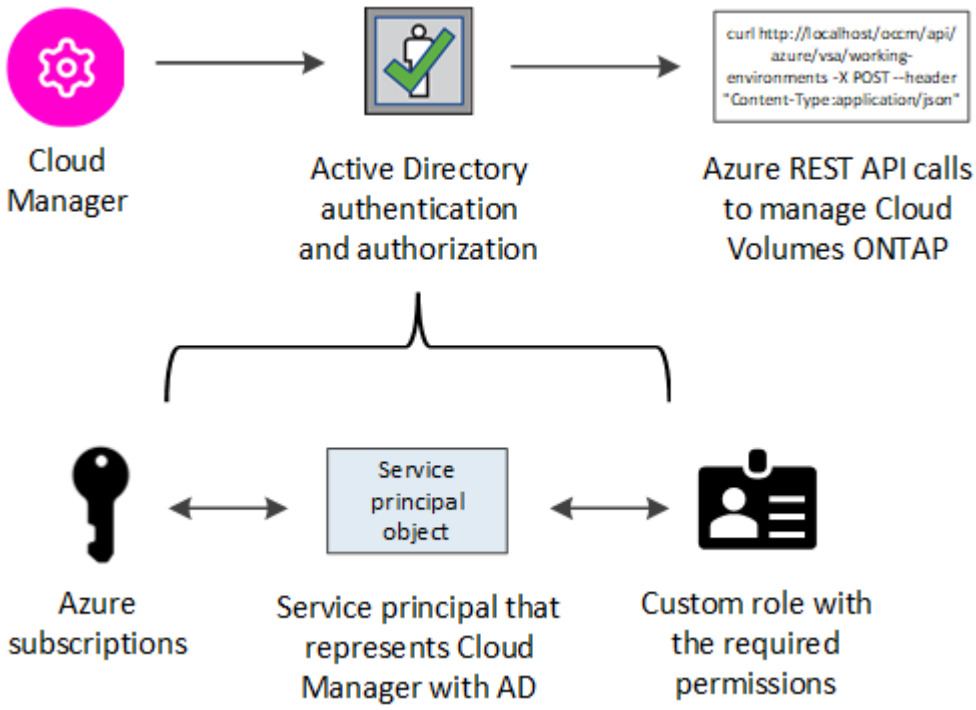
Cuando implementa un conector desde Cloud Manager, Cloud Manager agrega automáticamente la cuenta de Azure en la que implementó Connector. No se agrega una cuenta inicial si instaló manualmente el software Connector en un sistema existente. "Obtenga más información acerca de las cuentas y los permisos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

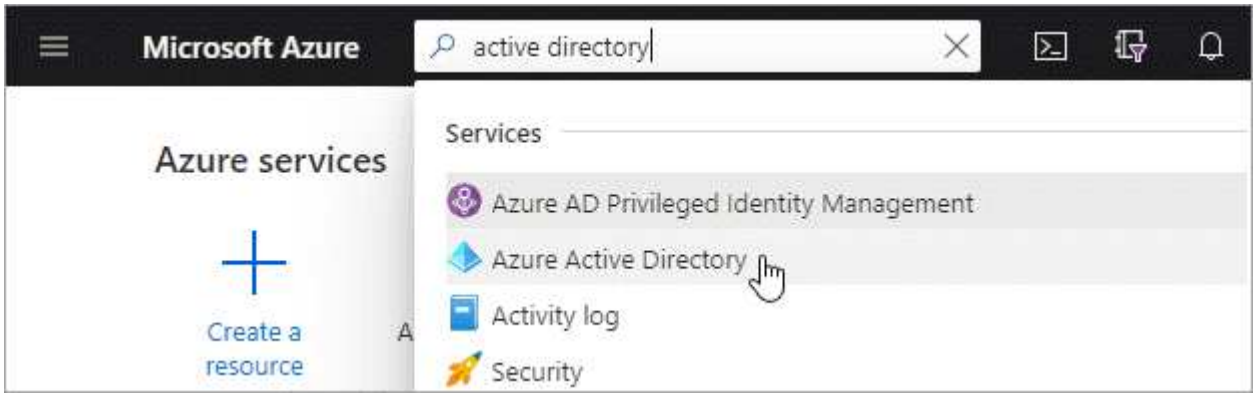
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que Cloud Manager pueda usar para el control de acceso basado en roles.

#### 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**.

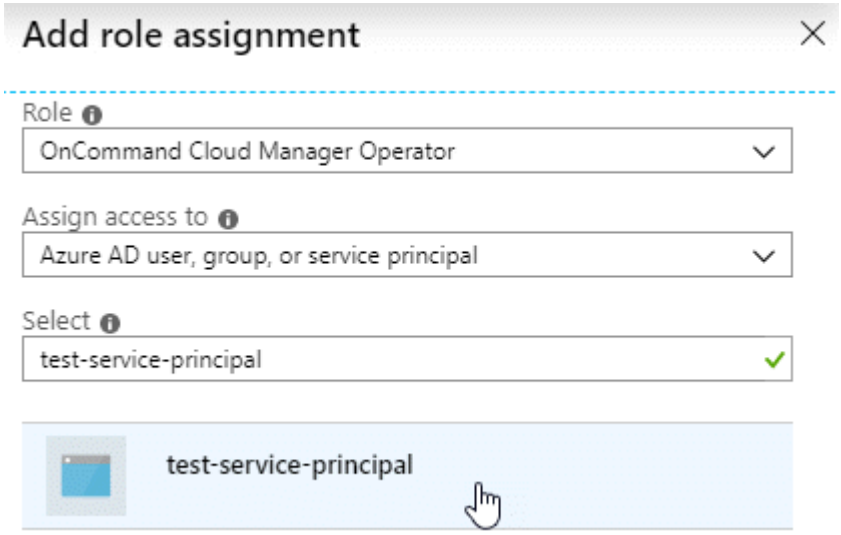
   b. Seleccione la suscripción.

   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.

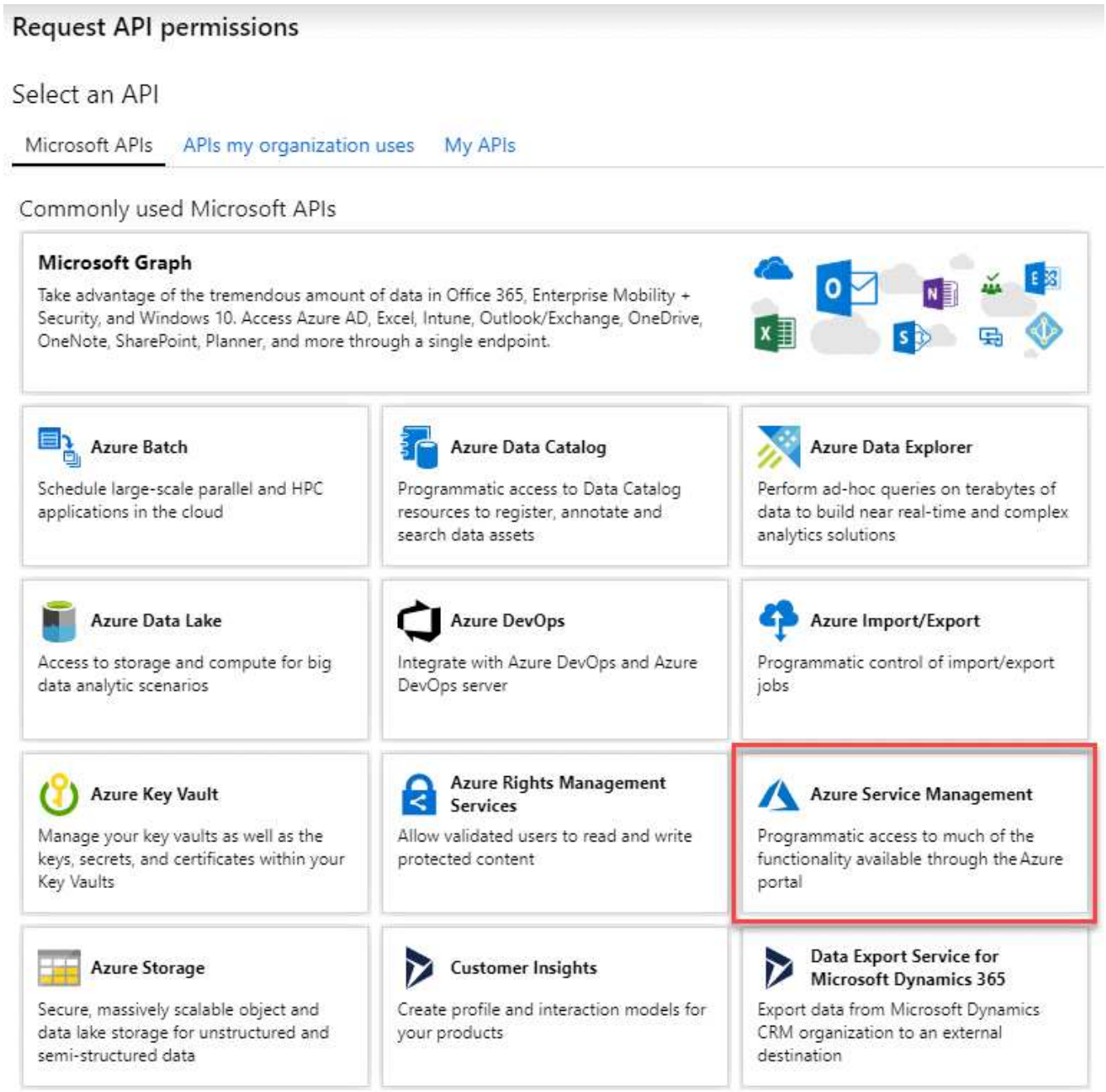
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. Cloud Manager le permite seleccionar la suscripción que desea utilizar al poner en marcha Cloud Volumes ONTAP.

#### Agregar permisos de API de administración de servicios de Windows Azure

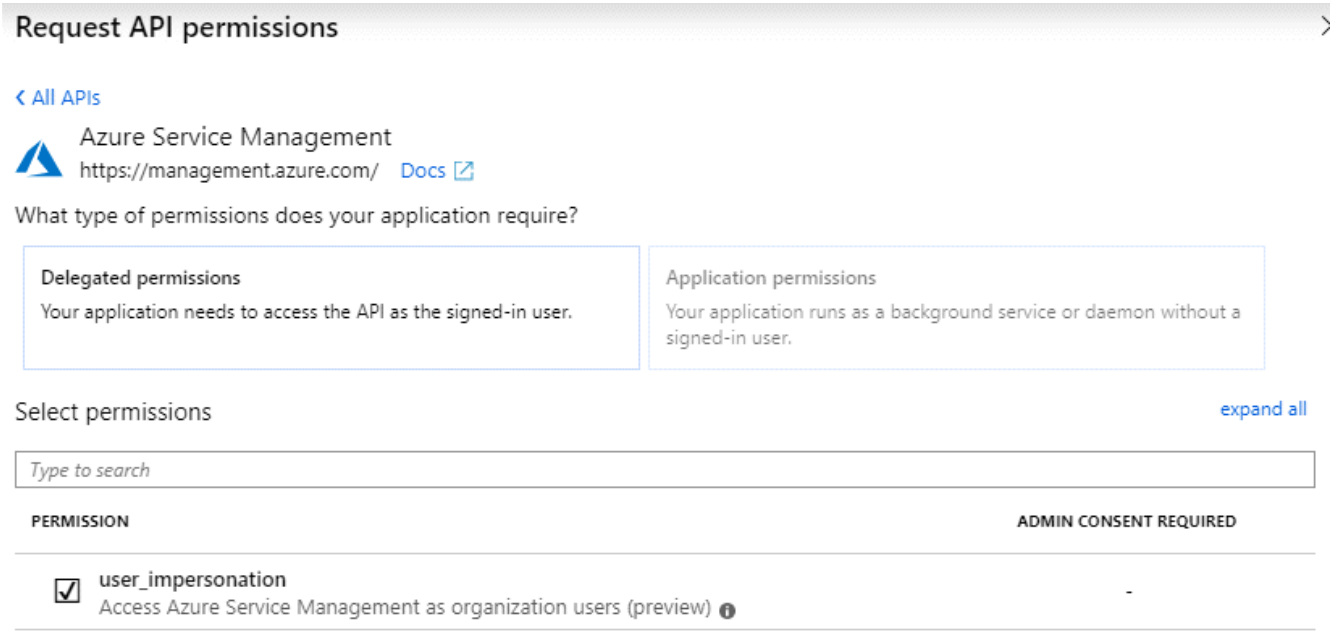
El principal de servicio debe tener permisos de "API de administración de servicios de Windows Azure".

**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**.

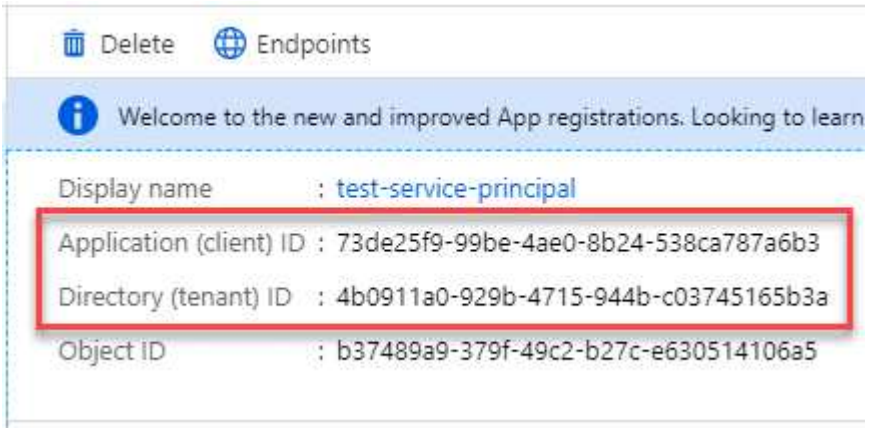



#### Obteniendo el ID de aplicación y el ID de directorio

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

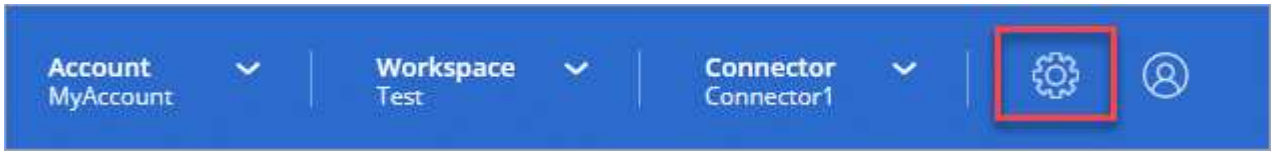
Después de proporcionar una cuenta de Azure con los permisos requeridos, puede añadir las credenciales para esa cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

**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**.



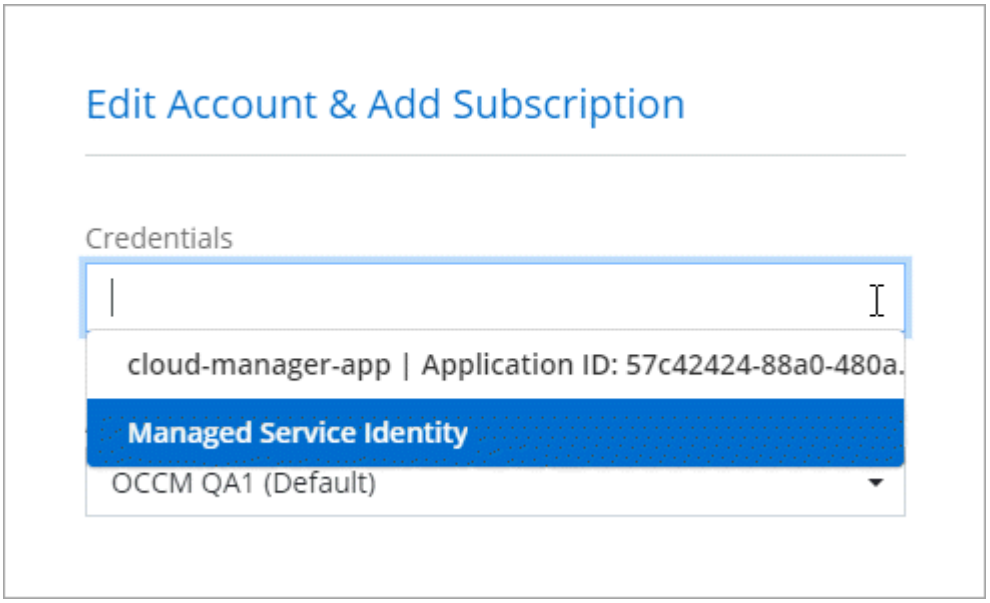

2. Haga clic en **Agregar credenciales** y seleccione **Microsoft Azure**.
3. Introduzca la información acerca del director del servicio de Azure Active Directory que otorga los permisos necesarios:
   - ID de aplicación (cliente): Consulte Obteniendo el ID de aplicación y el ID de directorio.
   - ID 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:

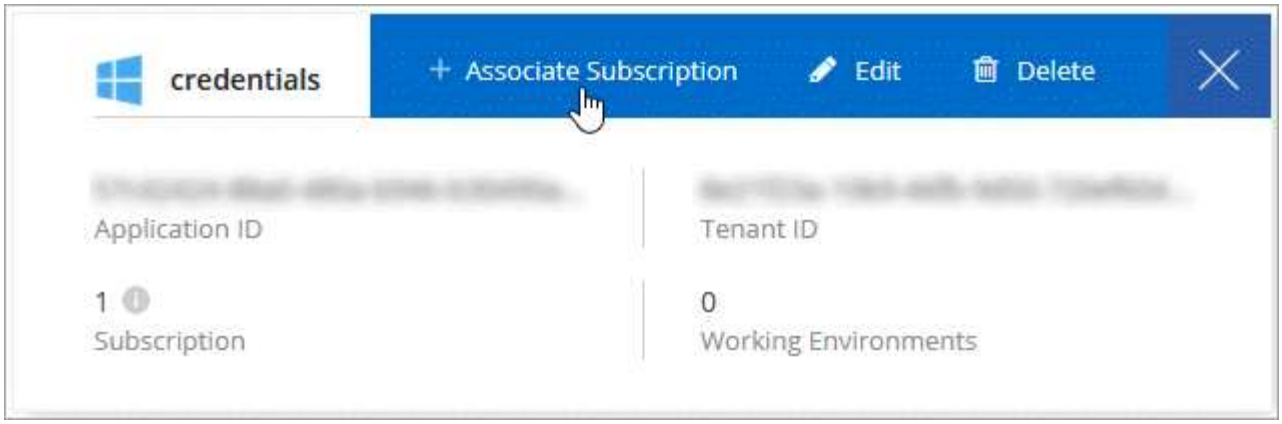
- No asoció una suscripción al agregar inicialmente las credenciales a Cloud Manager.
- Desea sustituir una suscripción existente de Azure Marketplace por una nueva suscripción.

**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

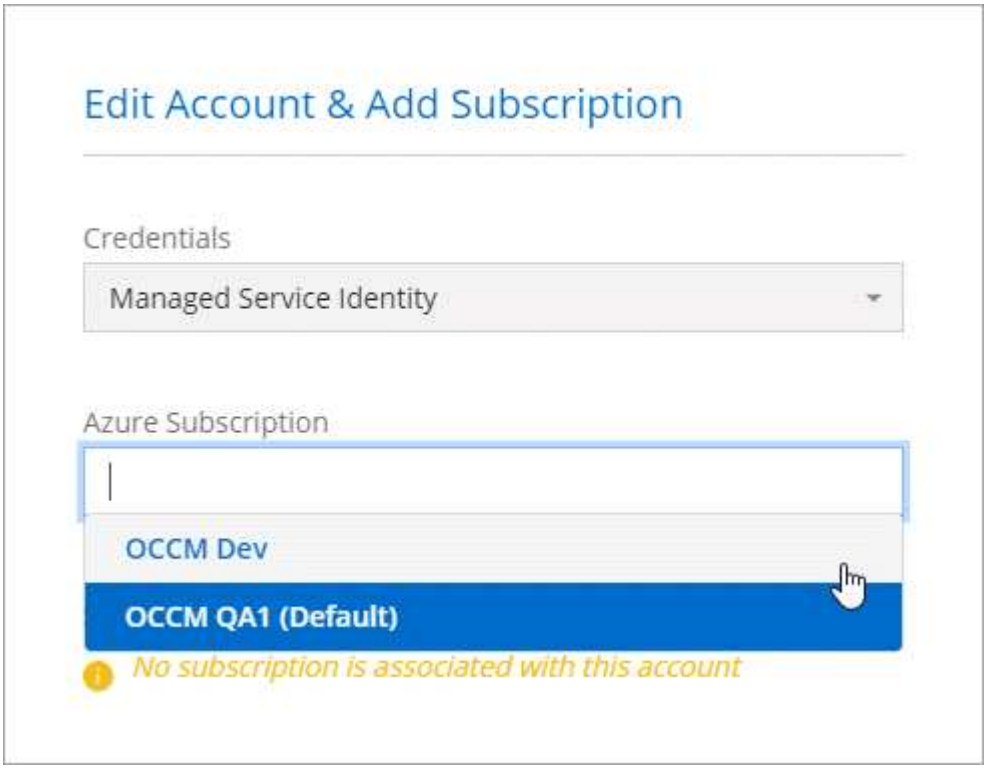
1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar Cloud Volumes ONTAP.
3. Haga clic en **Control de acceso (IAM)**.
   a. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos: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

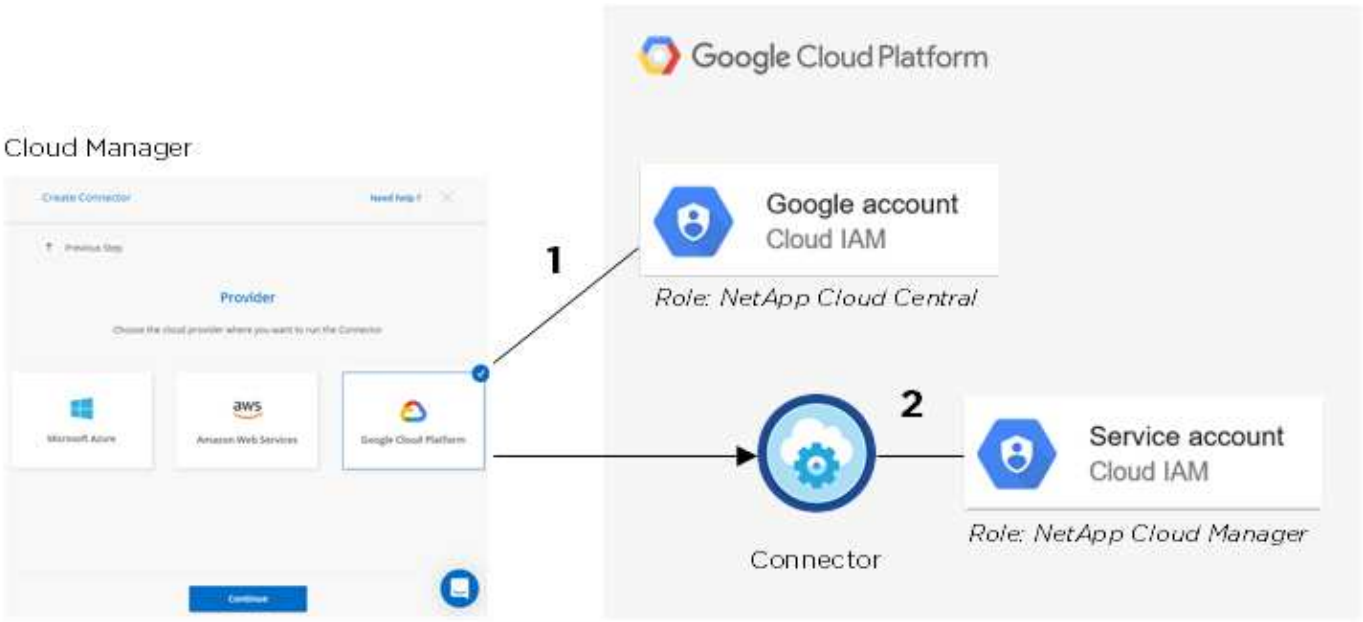
Debe haber dos conjuntos de permisos antes de implementar un conector directamente desde Cloud Manager:

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

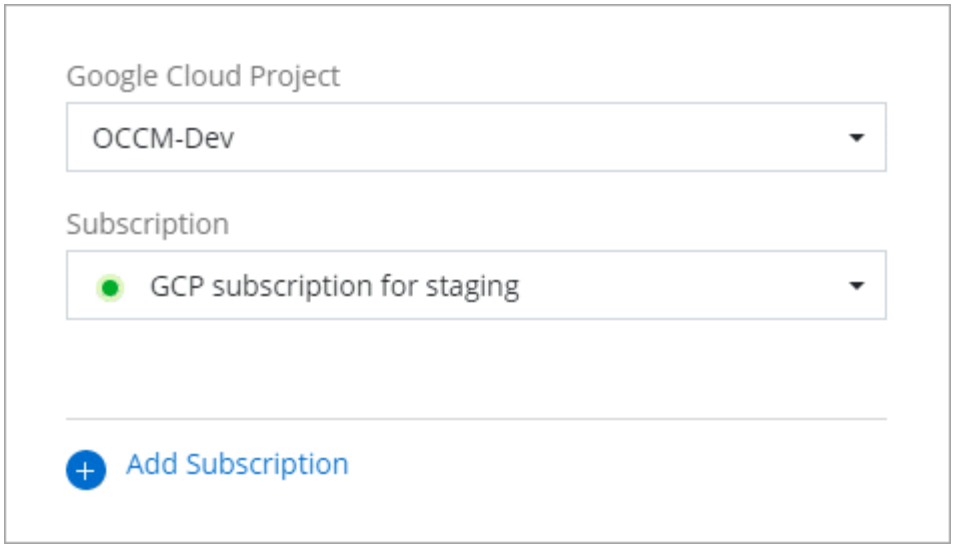
Al implementar un conector en GCP, Cloud Manager crea un conjunto predeterminado de credenciales asociadas con la instancia de Connector VM. Estas son las credenciales que utiliza Cloud Manager para poner en marcha Cloud Volumes ONTAP.

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.

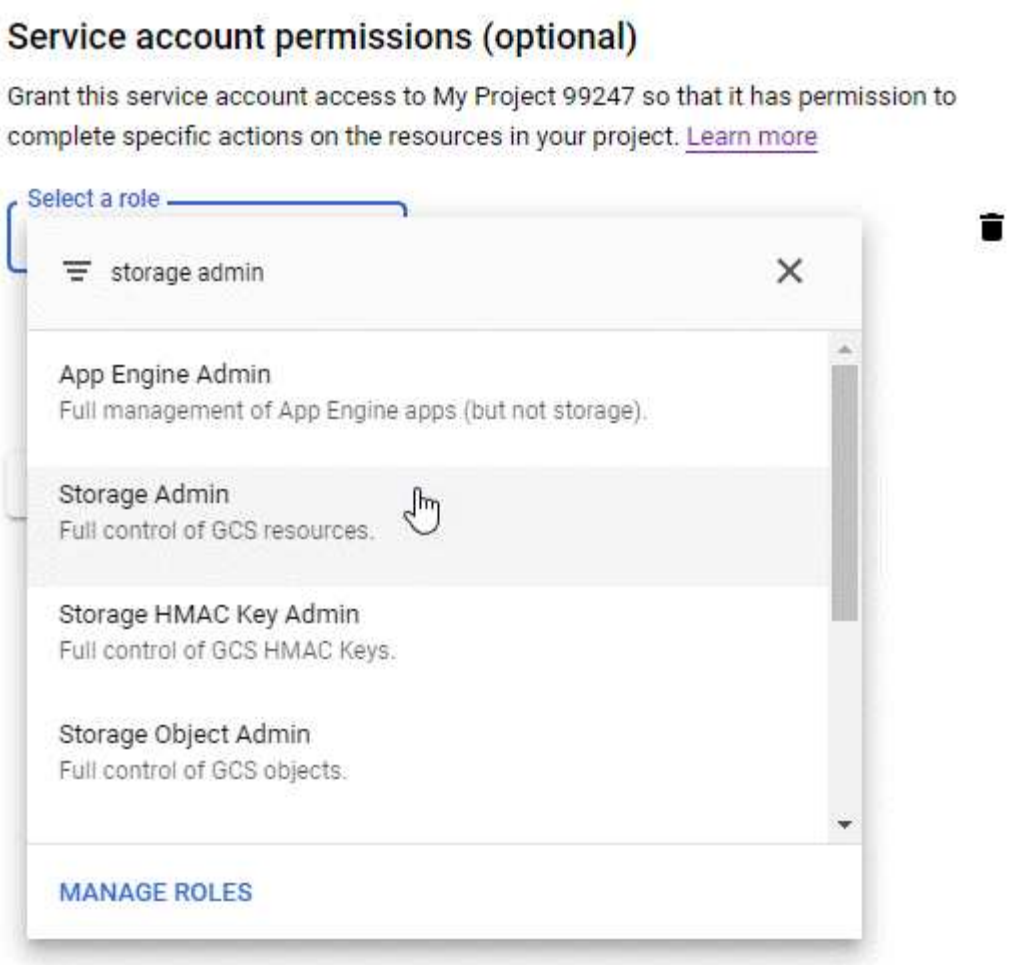
Si desea utilizar la organización en niveles de datos con Cloud Volumes ONTAP 9.7, siga el paso 4 en "Introducción a Cloud Volumes ONTAP en Google Cloud Platform".

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

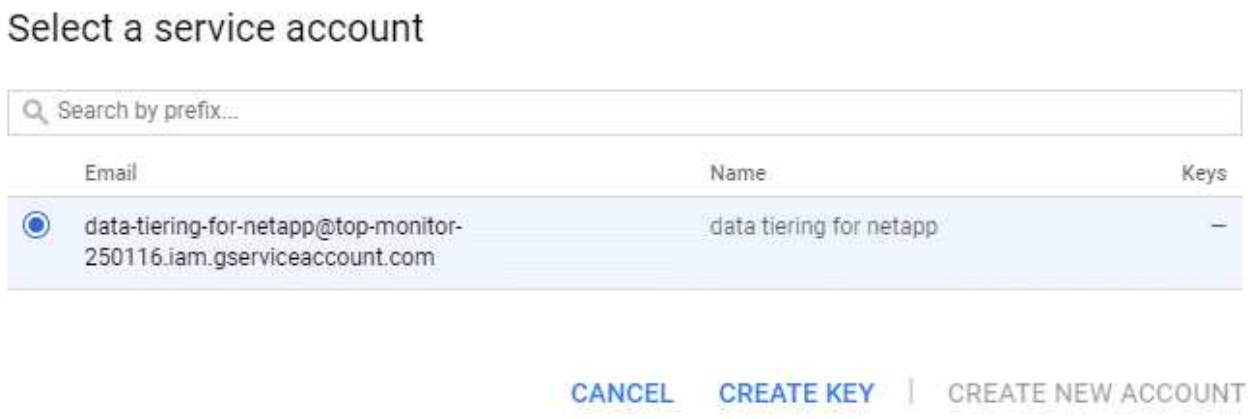
Una cuenta de servicio permite que Cloud Manager autentique y acceda a los bloques de almacenamiento en cloud que se utilizan para la organización en niveles de los datos. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

**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

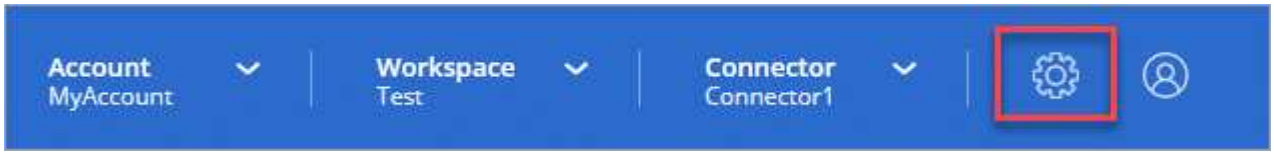
Ahora que tiene una clave de acceso para una cuenta de servicio, puede agregarla a Cloud Manager.

**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.

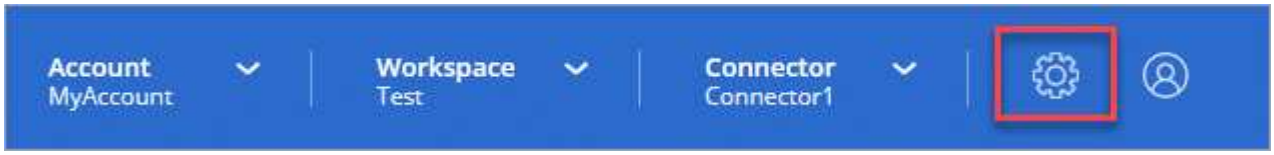
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

**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"

## Información de copyright



## Información de la marca comercial