



# Configure Cloud Manager

## Cloud Manager 3.7

NetApp  
March 25, 2024

# Tabla de contenidos

- Configure Cloud Manager ..... 1
  - Configuración de espacios de trabajo y usuarios en la cuenta de Cloud Central ..... 1
  - Configurar y añadir cuentas de AWS en Cloud Manager ..... 3
  - Configurar y añadir cuentas de Azure a Cloud Manager ..... 6
  - Configuración y adición de cuentas de GCP a Cloud Manager ..... 14
  - Adición de cuentas del sitio de soporte de NetApp a Cloud Manager ..... 17
  - Instalar un certificado HTTPS para obtener acceso seguro ..... 17
  - Configuración de AWS KMS ..... 19

# Configure Cloud Manager

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

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

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

### Agregar espacios de trabajo

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

#### Pasos

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



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

#### Después de terminar

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

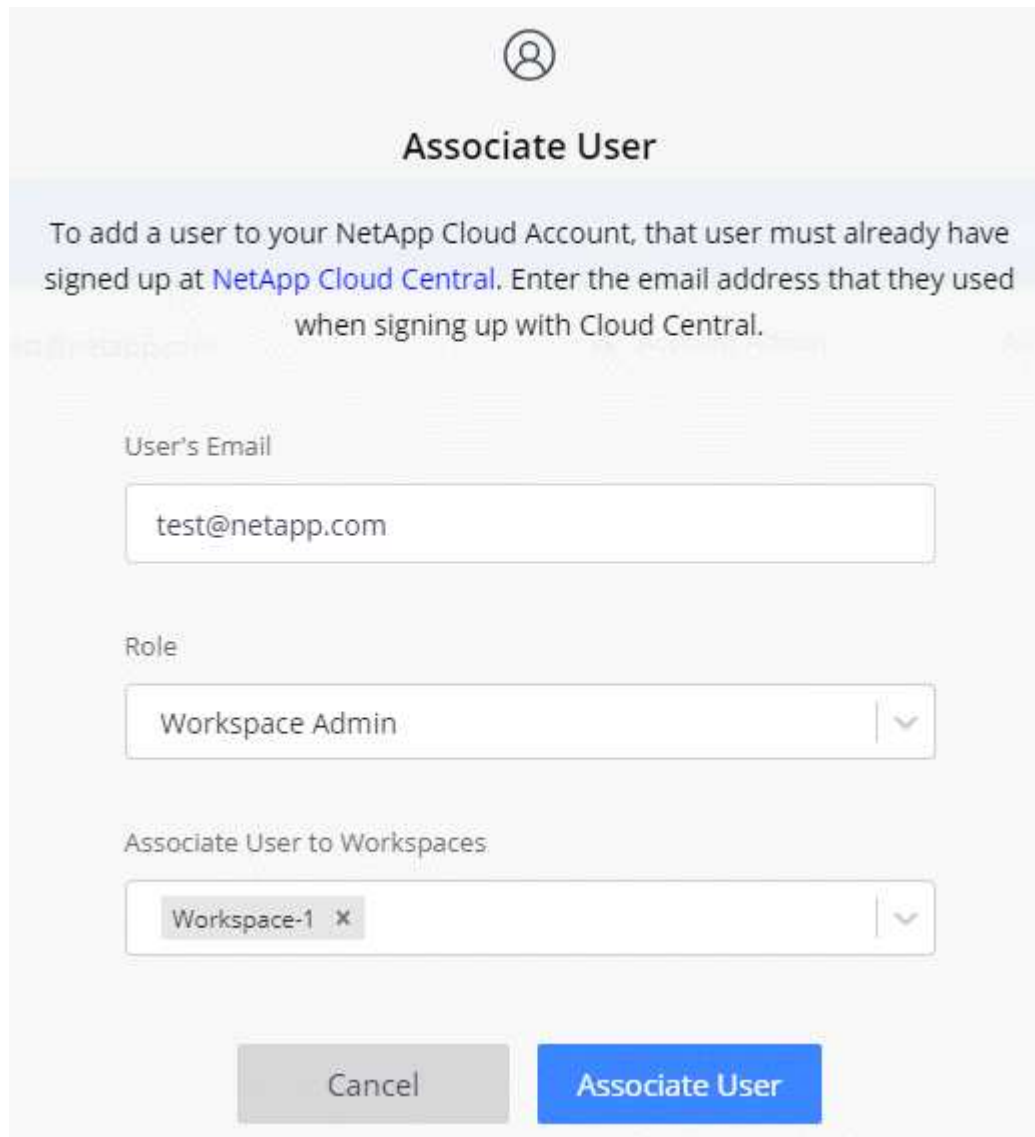
### Adición de usuarios

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

#### Pasos

1. Si el usuario aún no lo ha hecho, pida al usuario que vaya a ["Cloud Central de NetApp"](#) y crear una cuenta.
2. En Cloud Manager, haga clic en **Configuración de cuenta**.

3. En la ficha usuarios, haga clic en **Usuario asociado**.
4. Introduzca la dirección de correo electrónico del usuario y seleccione un rol para el usuario:
  - **Administrador de cuentas:** Puede realizar cualquier acción en Cloud Manager.
  - **Administración de área de trabajo:** Puede crear y administrar recursos en áreas de trabajo asignadas.
5. Si ha seleccionado Administrador de área de trabajo, seleccione una o más áreas de trabajo para asociarlas a ese usuario.



**Associate User**

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

Role

Associate User to Workspaces

Cancel Associate User

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

### Resultado

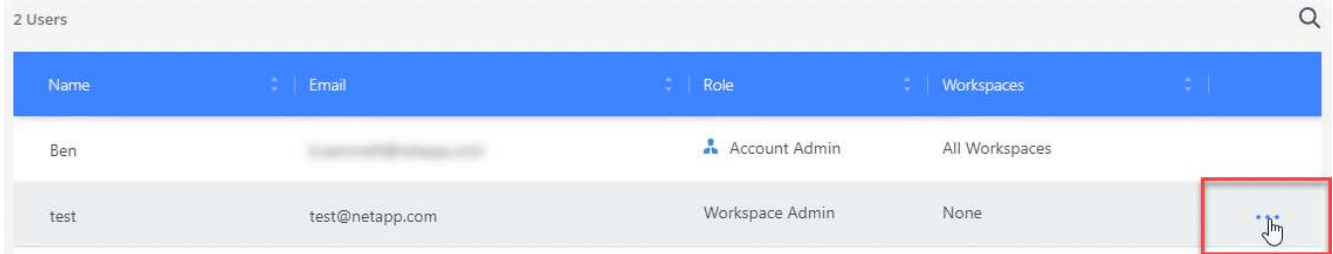
El usuario debe recibir un correo electrónico de Cloud Central de NetApp titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a Cloud Manager.

### Asociación de administradores de área de trabajo con áreas de trabajo

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

## Pasos

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



Name	Email	Role	Workspaces
Ben		Account Admin	All Workspaces
test	test@netapp.com	Workspace Admin	None

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

## Resultado

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

## Asociación de conectores de servicio con áreas de trabajo

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

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

["Obtenga más información sobre usuarios, espacios de trabajo y conectores de servicio"](#).

## Pasos

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

## Resultado

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

## Configurar y añadir cuentas de AWS en Cloud Manager

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



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

## opciones

- [Concesión de permisos proporcionando claves AWS](#)
- [Otorgar permisos asumiendo roles de IAM en otras cuentas](#)

## Concesión de permisos proporcionando claves AWS

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

### Pasos

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

["Documentación de AWS: Crear políticas de IAM"](#)

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

### Resultado

La cuenta ahora tiene los permisos necesarios. [Ahora puede añadirlo a Cloud Manager](#).

## Otorgar permisos asumiendo roles de IAM en otras cuentas

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

### Pasos

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

No olvide hacer lo siguiente:

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

## Create role



### Select type of trusted entity

Four options for trusted entity type are shown in a row:

- AWS service**: EC2, Lambda and others.
- Another AWS account**: Belonging to you or 3rd party. This option is highlighted with a blue border.
- Web identity**: Cognito or any OpenID provider.
- SAML 2.0 federation**: Your corporate directory.

Allows entities in other accounts to perform actions in this account. [Learn more](#)

### Specify accounts that can use this role

Account ID\*  ⓘ

- Options
- Require external ID (Best practice when a third party will assume this role)
  - Require MFA ⓘ

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

- Haga clic en **Relaciones de confianza > Editar relación de confianza**.
- Agregue la acción "sts:AssumeRole" y el ARN de la función que creó en la cuenta de destino.

### ejemplo

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

### Resultado

La cuenta ahora tiene los permisos necesarios. [Ahora puede añadirlo a Cloud Manager](#).

## Añadiendo cuentas de AWS a Cloud Manager

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

### Pasos

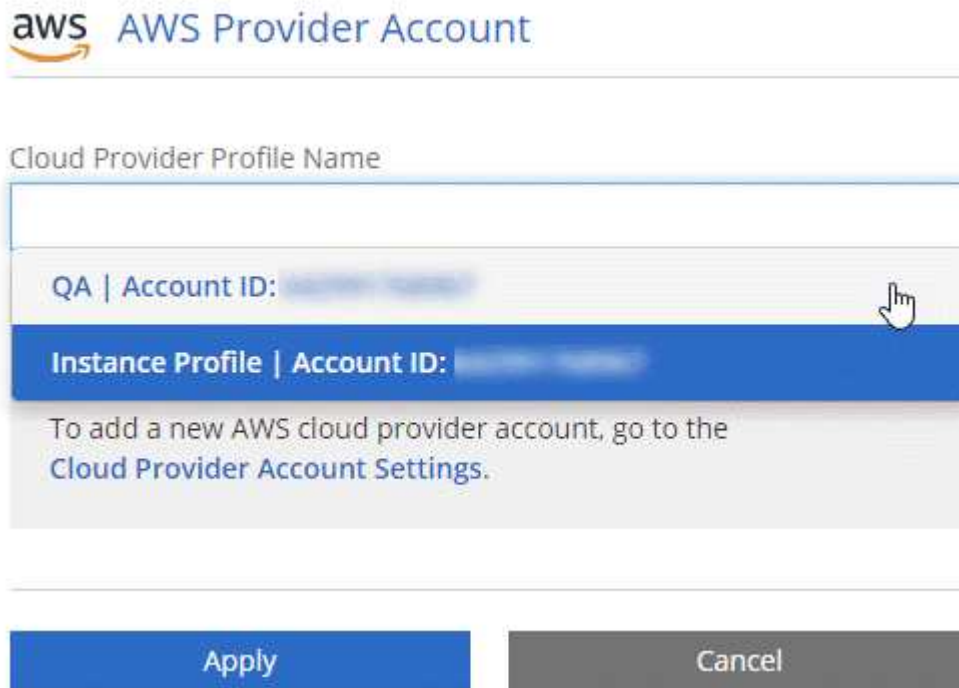
- En la esquina superior derecha de la consola de Cloud Manager, haga clic en el icono Configuración y seleccione **Proveedor de cloud y Cuentas de soporte**.



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

### Resultado

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



## Configurar y añadir cuentas de Azure a Cloud Manager

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



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

### Concesión de permisos de Azure con un director de servicio

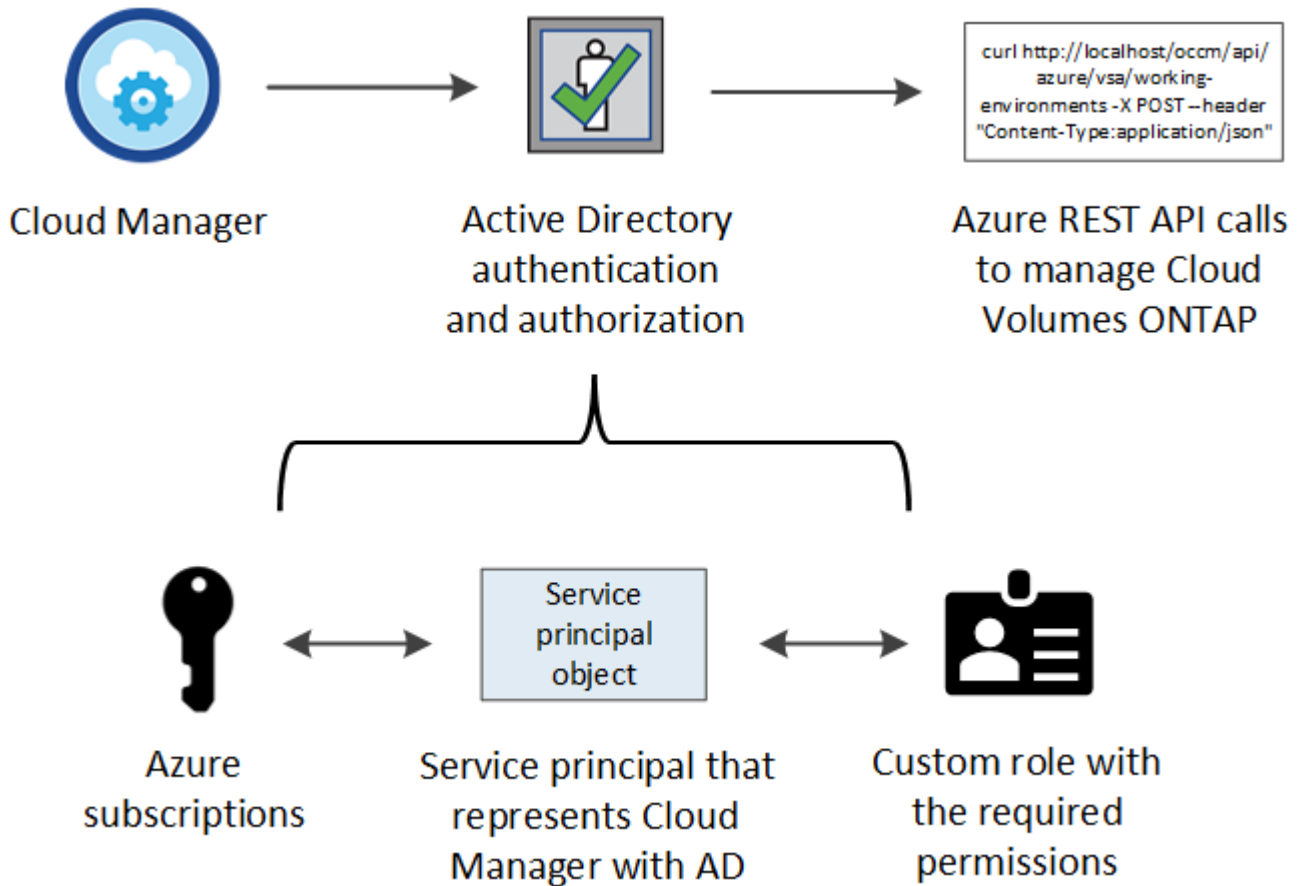
Cloud Manager necesita permisos para realizar acciones en Azure. Puede conceder los permisos requeridos a una cuenta de Azure creando y configurando un servicio principal en Azure Active Directory y obteniendo las credenciales de Azure que necesita Cloud Manager.

#### Acerca de esta tarea

La siguiente imagen muestra cómo Cloud Manager obtiene permisos para realizar operaciones en Azure. Un



objeto principal de servicio, que está vinculado a una o varias suscripciones de Azure, representa Cloud Manager en Azure Active Directory y se asigna a una función personalizada que permite los permisos necesarios.



## Pasos

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

## Crear una aplicación de Azure Active Directory

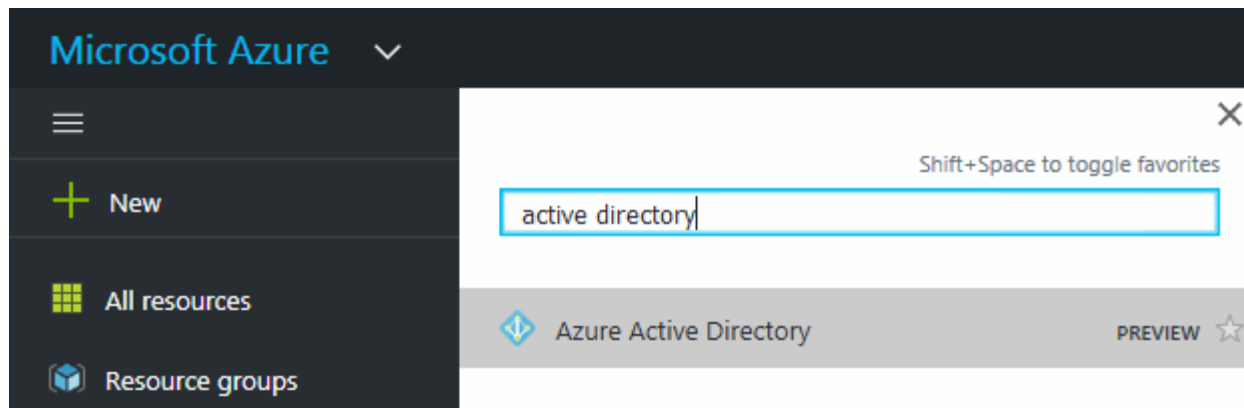
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que Cloud Manager pueda usar para el control de acceso basado en roles.

### Antes de empezar

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

## Pasos

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



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

### Resultado

Ha creado la aplicación AD y el director de servicio.

### Asignación de la aplicación a una función

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

### Pasos

1. Crear un rol personalizado:
  - a. Descargue el "[Política de Azure de Cloud Manager](#)".
  - b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

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

### ejemplo

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

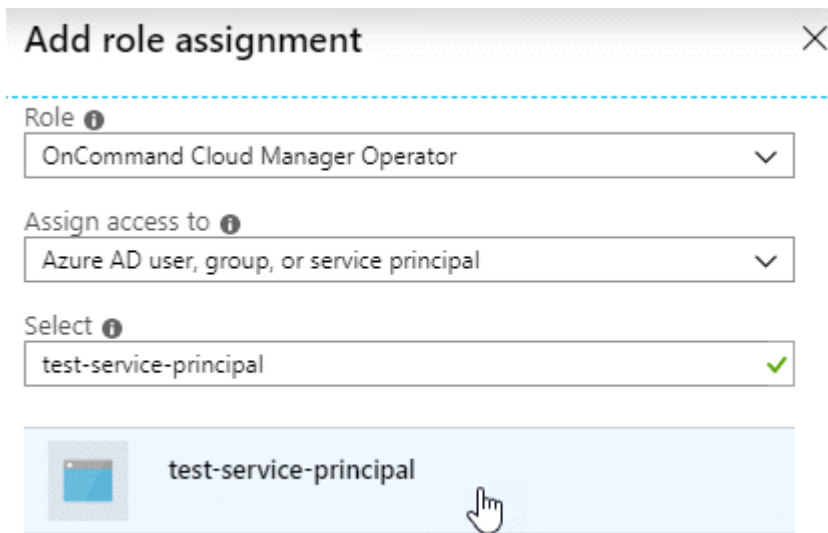
- c. Use el archivo JSON para crear una función personalizada en Azure.

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

## Az role definition create --role-definition C:\Policy\_for\_cloud\_Manager\_Azure\_3.7.4.json

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

2. Asigne la aplicación al rol:
  - a. En el portal de Azure, abra el servicio **Suscripciones**.
  - b. Seleccione la suscripción.
  - c. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
  - d. Seleccione el rol **operador de Cloud Manager de OnCommand**.
  - e. Mantener seleccionado **usuario, grupo o principal de servicio de Azure AD**.
  - f. Busque el nombre de la aplicación (no puede encontrarlo en la lista desplazándose).



The screenshot shows the 'Add role assignment' dialog box. It has a title bar with a close button (X). Below the title bar, there are three dropdown menus. The first is labeled 'Role' and has 'OnCommand Cloud Manager Operator' selected. The second is labeled 'Assign access to' and has 'Azure AD user, group, or service principal' selected. The third is labeled 'Select' and has 'test-service-principal' selected, with a green checkmark to its right. Below these dropdowns, there is a search bar containing 'test-service-principal' and a blue button with a hand cursor pointing to it.

- 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**.

## Request API permissions

Select an API

[Microsoft APIs](#) [APIs my organization uses](#) [My APIs](#)


Commonly used Microsoft APIs

<b>Microsoft Graph</b> Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint. 		
<b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud	<b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	<b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
<b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios	<b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server	<b>Azure Import/Export</b> Programmatic control of import/export jobs
<b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	<b>Azure Rights Management Services</b> Allow validated users to read and write protected content	<b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal
<b>Azure Storage</b> Secure, massively scalable object and data lake storage for unstructured and semi-structured data	<b>Customer Insights</b> Create profile and interaction models for your products	<b>Data Export Service for Microsoft Dynamics 365</b> Export data from Microsoft Dynamics CRM organization to an external destination

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

## Request API permissions

[< All APIs](#)

 Azure Service Management  
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

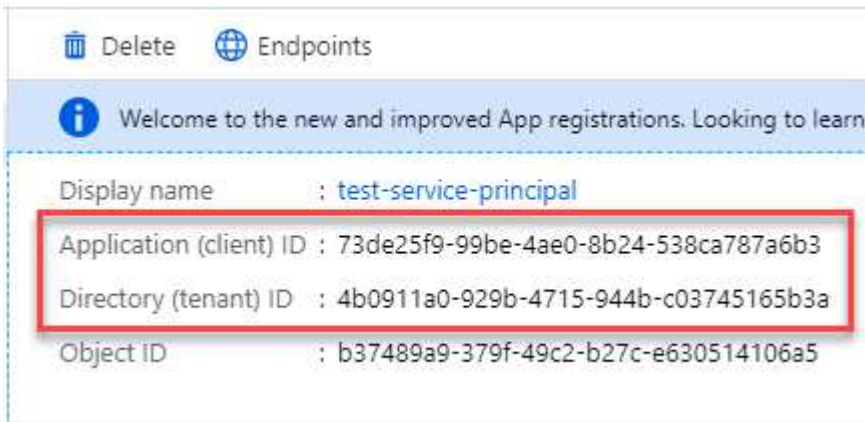
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) 	-

## 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)**.



Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

## 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 registros** 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.

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRov4NLfdAcY7:+0vA	

### Resultado

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

## Adición de cuentas de Azure a Cloud Manager

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

### Pasos

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



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

### Resultado

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



Cloud Provider Profile Name

Azure Keys | Application ID: [redacted] ...  
Dev Keys | Application ID: [redacted] ...  
**Managed Service Identity**

To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).

Apply

Cancel

## Asociar suscripciones de Azure adicionales a una identidad administrada

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

### Acerca de esta tarea

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

### Pasos

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



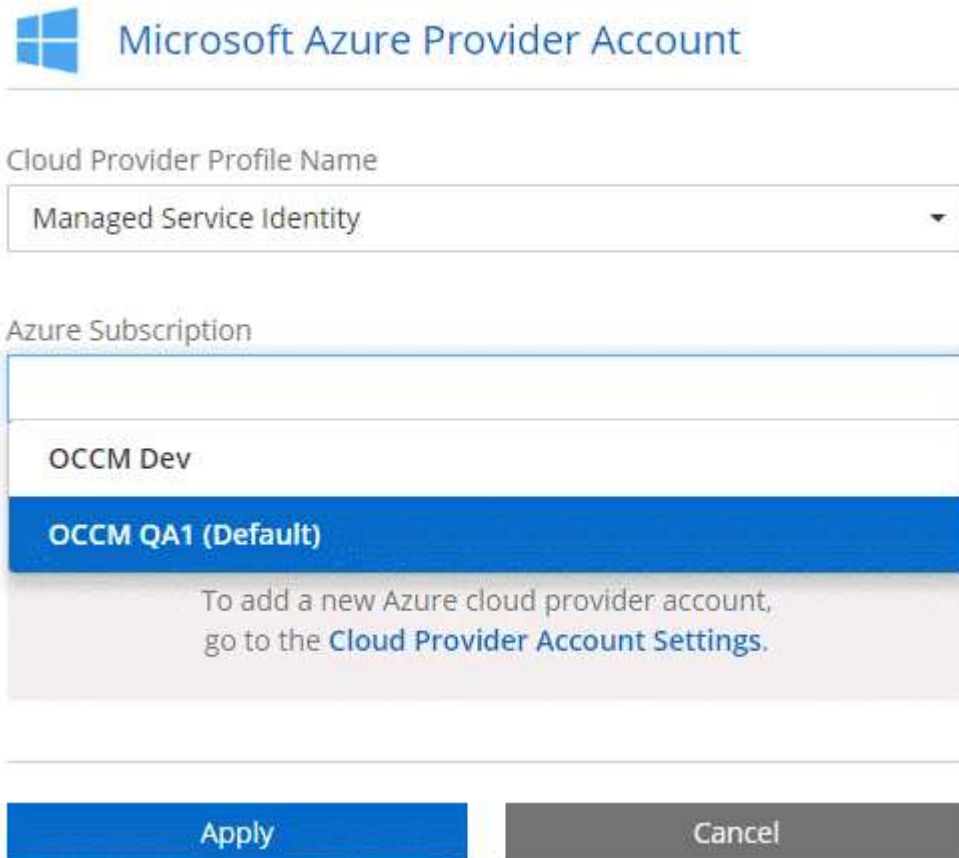
El nombre predeterminado que se proporciona en la es el operador de OnCommand Cloud Manager "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

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

4. Repita estos pasos para suscripciones adicionales.

### Resultado

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



The screenshot shows the 'Microsoft Azure Provider Account' configuration page. At the top, there is a Microsoft logo and the title 'Microsoft Azure Provider Account'. Below this, there is a section for 'Cloud Provider Profile Name' with a dropdown menu currently set to 'Managed Service Identity'. Underneath is the 'Azure Subscription' section, which contains a list of subscriptions. The first subscription is 'OCCM Dev', and the second is 'OCCM QA1 (Default)', which is highlighted in blue. Below the list, there is a message: 'To add a new Azure cloud provider account, go to the [Cloud Provider Account Settings](#).' At the bottom of the form, there are two buttons: 'Apply' (in blue) and 'Cancel' (in grey).

## Configuración y adición de cuentas de GCP a Cloud Manager

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



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

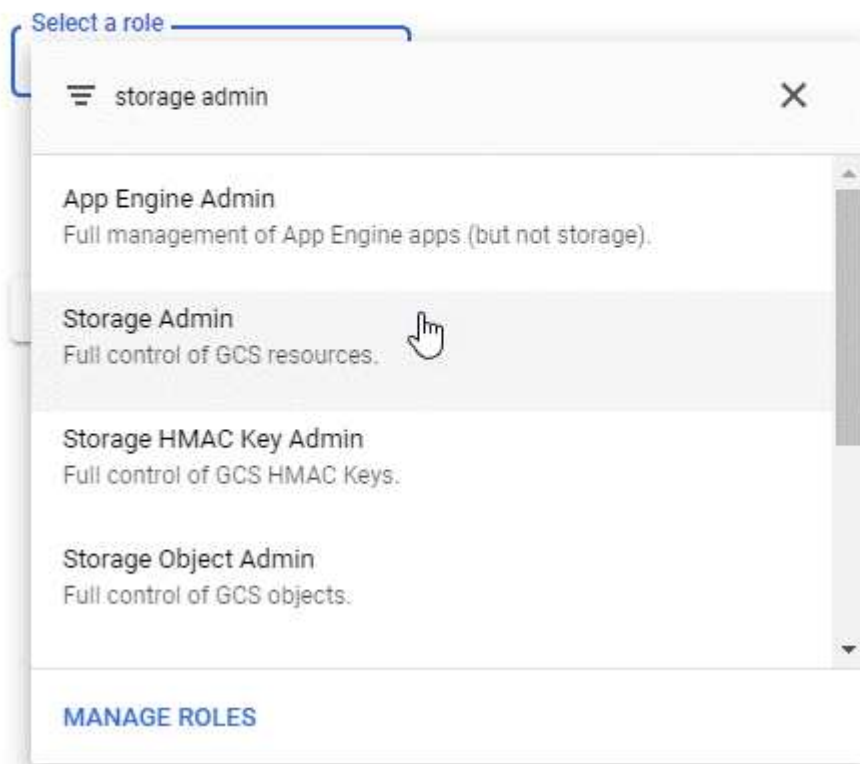
Una cuenta de servicio permite que Cloud Manager autentique y acceda a los bloques de almacenamiento en cloud que se utilizan para la organización en niveles de los datos. Las claves son necesarias para que Google Cloud Storage sepa quién está haciendo la solicitud.

### Pasos

1. Abra la consola GCP IAM y. "[Cree una cuenta de servicio con el rol Storage Admin](#)".

### Service account permissions (optional)

Grant this service account access to My Project 99247 so that it has permission to complete specific actions on the resources in your project. [Learn more](#)



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.

## Select a service account

Search by prefix...

Email	Name	Keys
<input checked="" type="radio"/> data-tiering-for-netapp@top-monitor-250116.iam.gserviceaccount.com	data tiering for netapp	—

CANCEL CREATE KEY | CREATE NEW ACCOUNT

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

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

## Añadir una cuenta de GCP a Cloud Manager

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

### Pasos

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



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

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

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

### El futuro

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

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

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

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

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

📺 | <https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg>

## Pasos

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



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

## El futuro

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

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

## Instalar un certificado HTTPS para obtener acceso seguro

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

## Pasos

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



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

Opción	Descripción
Genere una CSR	<ol style="list-style-type: none"> <li>a. Introduzca el nombre de host o DNS del host de Cloud Manager (su nombre común) y, a continuación, haga clic en <b>generar CSR</b>.  Cloud Manager muestra una solicitud de firma de certificación.</li> <li>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.</li> <li>c. Copie el contenido del certificado firmado, péguelo en el campo Certificado y, a continuación, haga clic en <b>instalar</b>.</li> </ol>
Instale su propio certificado firmado por CA	<ol style="list-style-type: none"> <li>a. Seleccione <b>instalar certificado firmado por CA</b>.</li> <li>b. Cargue el archivo de certificado y la clave privada y, a continuación, haga clic en <b>instalar</b>.  El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.</li> </ol>

### 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:

## Cloud Manager HTTPS certificate

Expiration:

⚠ Oct 27, 2016 05:13:28 am

Issuer:

CN=localhost, O=NetApp, OU=Tel-Aviv,  
EMAILADDRESS=admin@example.com

Subject:

EMAILADDRESS=admin@example.com,  
OU=Tel-Aviv, O=NetApp, CN=localhost

 [View Certificate](#)

 [Renew HTTPS Certificate](#)

## Configuración de AWS KMS

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

### Pasos

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

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

["Documentación de AWS: Claves maestras de clientes \(CMKs\)"](#)

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

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

["Documentación de AWS: Editar claves"](#)

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

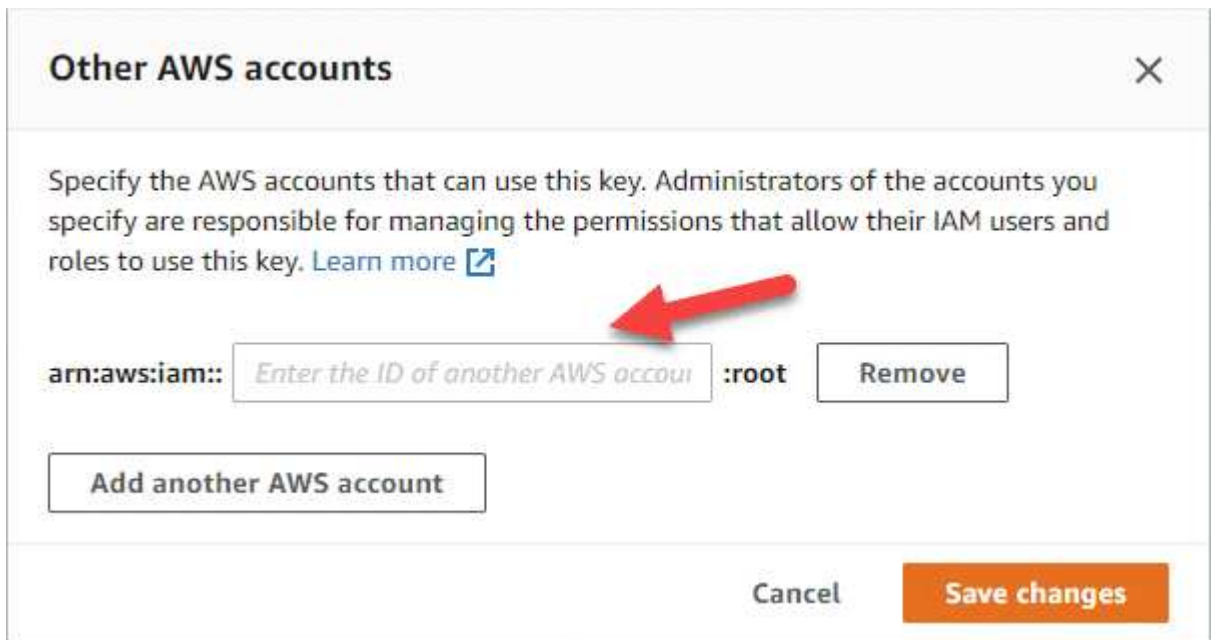
- a. Vaya a la consola KMS desde la cuenta donde reside el CMK.
- b. Seleccione la tecla.
- c. En el panel **Configuración general**, copie el ARN de la clave.

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

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

En la mayoría de los casos, esta es la cuenta en la que reside Cloud Manager. Si Cloud Manager no

se instaló en AWS, sería la cuenta para la que proporcionó las claves de acceso de AWS a Cloud Manager.



- e. Cambie ahora a la cuenta de AWS que proporciona permisos a Cloud Manager y abra la consola IAM.
- f. Cree una política de IAM que incluya los permisos que se indican a continuación.
- g. Asocie la política al rol de IAM o al usuario IAM que proporciona permisos a Cloud Manager.

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

```

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

```

+

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

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.