



# **Configurar Cloud Manager**

## **Cloud Manager 3.6**

NetApp  
March 25, 2024

This PDF was generated from [https://docs.netapp.com/es-es/occm36/task\\_adding\\_cloud\\_accounts.html](https://docs.netapp.com/es-es/occm36/task_adding_cloud_accounts.html) on March 25, 2024. Always check docs.netapp.com for the latest.

# Tabla de contenidos

- Configurar Cloud Manager ..... 1
  - Añadiendo cuentas de proveedores de cloud a Cloud Manager ..... 1
  - Adición de cuentas del sitio de soporte de NetApp a Cloud Manager ..... 10
  - Instalar un certificado HTTPS para obtener acceso seguro ..... 11
  - Configurar usuarios e inquilinos ..... 12
  - Configuración de AWS KMS ..... 13

# Configurar Cloud Manager

## Añadiendo cuentas de proveedores de cloud a Cloud Manager

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

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

### Configurar y añadir cuentas de AWS en Cloud Manager

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

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

#### Concesión de permisos al proporcionar claves AWS

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

##### Pasos

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

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

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

##### Resultado

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

#### Otorgar permisos asumiendo roles de IAM en otras cuentas

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

##### Pasos

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

No olvide hacer lo siguiente:

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

## Create role




### Select type of trusted entity

 <b>AWS service</b> EC2, Lambda and others	 <b>Another AWS account</b> Belonging to you or 3rd party	 <b>Web identity</b> Cognito or any OpenID provider	 <b>SAML 2.0 federation</b> 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.

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

### ejemplo

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

### Resultado

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

### Añadiendo cuentas de AWS a Cloud Manager

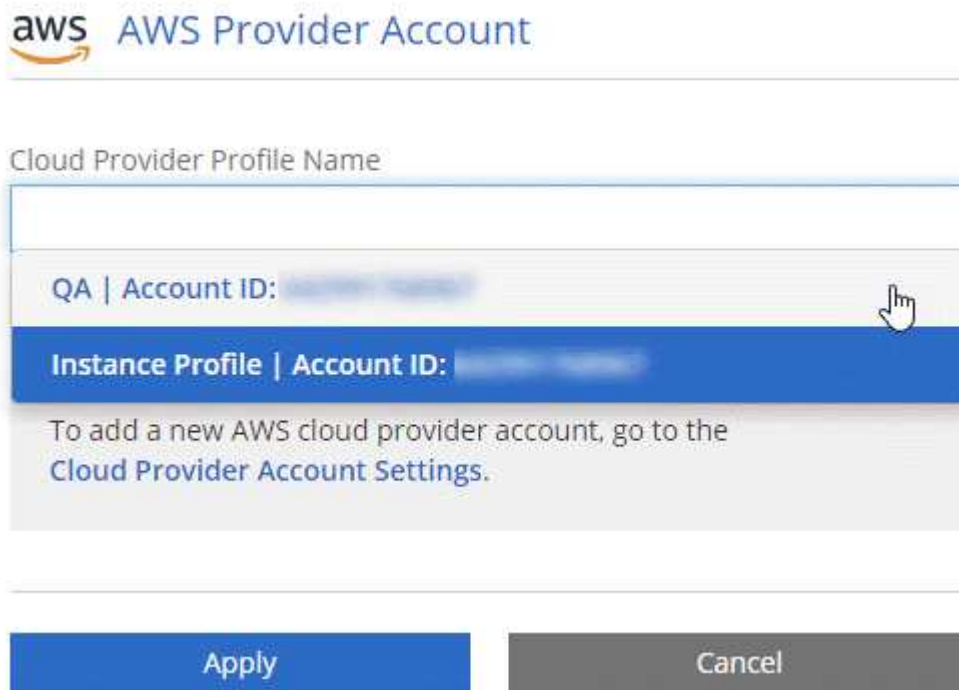
Después de proporcionar una cuenta de AWS con los permisos necesarios, puede añadir la cuenta a Cloud Manager. Esto le permite iniciar sistemas de Cloud Volumes ONTAP en esa cuenta.

## Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en la lista desplegable de tareas y, a continuación, seleccione **Configuración de cuenta**.
2. Haga clic en **Agregar nueva cuenta** y seleccione **AWS**.
3. Elija si desea proporcionar las claves AWS o el ARN de un rol de IAM de confianza.
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **Crear cuenta**.

## Resultado

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



## Configurar y añadir cuentas de Azure a Cloud Manager

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

- [Concesión de permisos de Azure con un director de servicio](#)
- [Adición de cuentas de Azure a Cloud Manager](#)

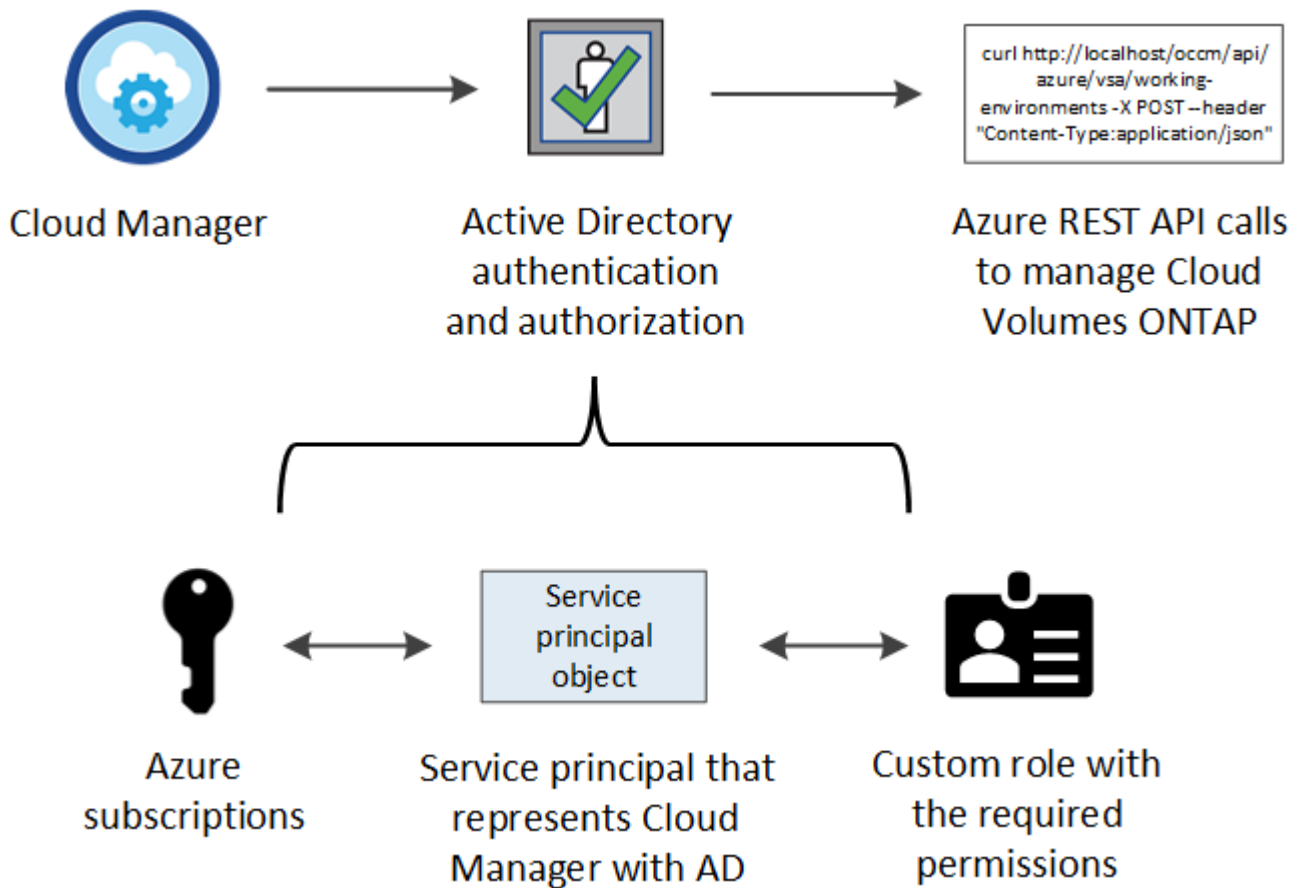
### Concesión de permisos de Azure con un director de servicio

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

### Acerca de esta tarea

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

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



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

#### Pasos

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

#### Crear un rol personalizado con los permisos de Cloud Manager necesarios

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

#### Pasos

1. Descargue el "[Política de Azure de Cloud Manager](#)".
2. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

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

#### ejemplo

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

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

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

**Az role definition create --role-definition C:\Policy\_for\_cloud\_Manager\_Azure\_3.6.1.json**

## Resultado

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

## Creación de una entidad de servicio de Active Directory

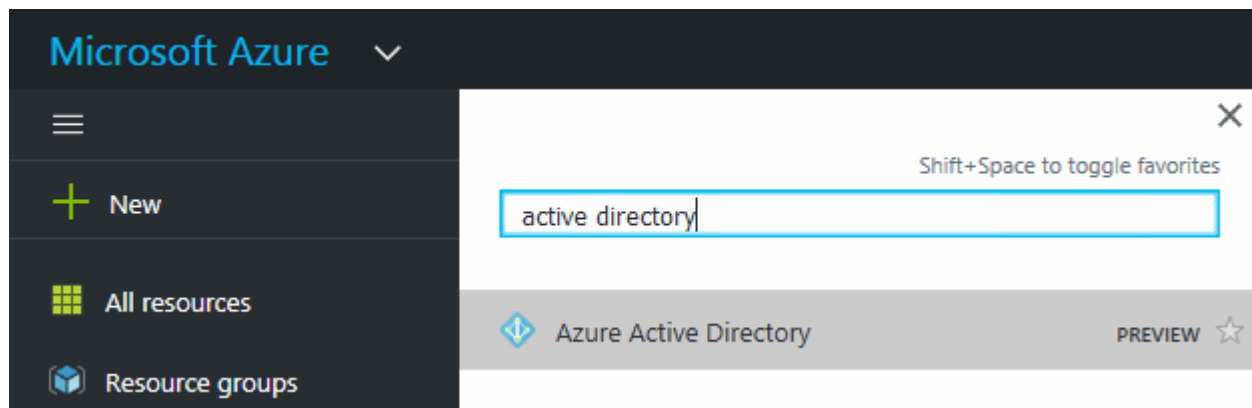
Debe crear un director de servicio de Active Directory para que Cloud Manager se pueda autenticar con Azure Active Directory.

## Antes de empezar

Debe tener los permisos adecuados en Azure para crear una aplicación de Active Directory y asignar la aplicación a un rol. Para obtener más información, consulte ["Documentación de Microsoft Azure: Utilice el portal para crear una aplicación de Active Directory y una entidad de servicio con acceso a los recursos"](#).

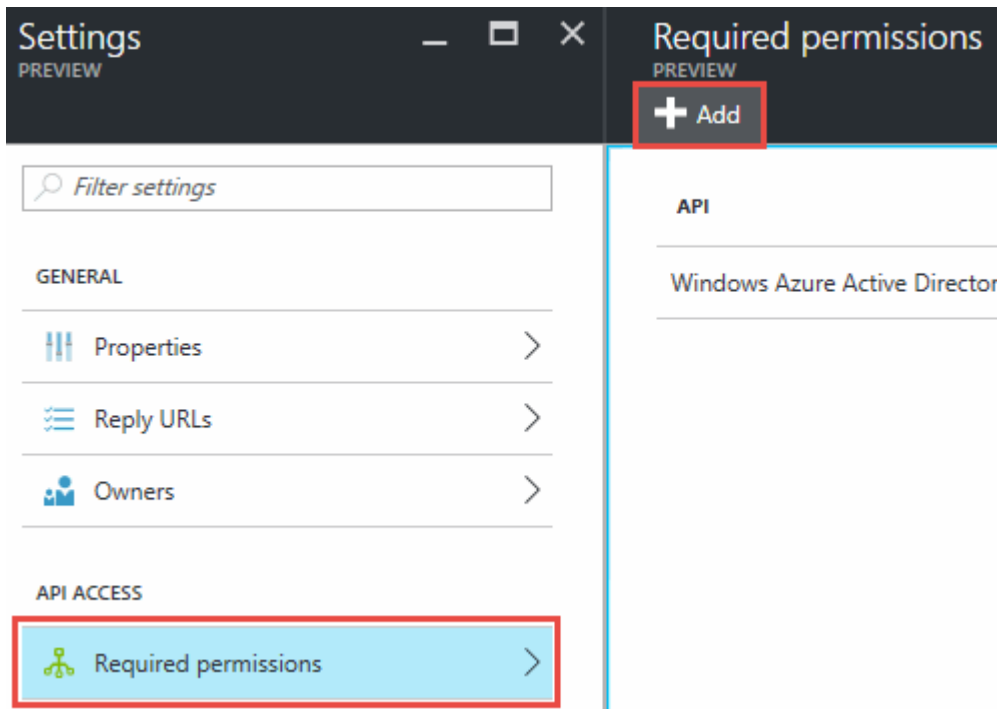
## Pasos

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

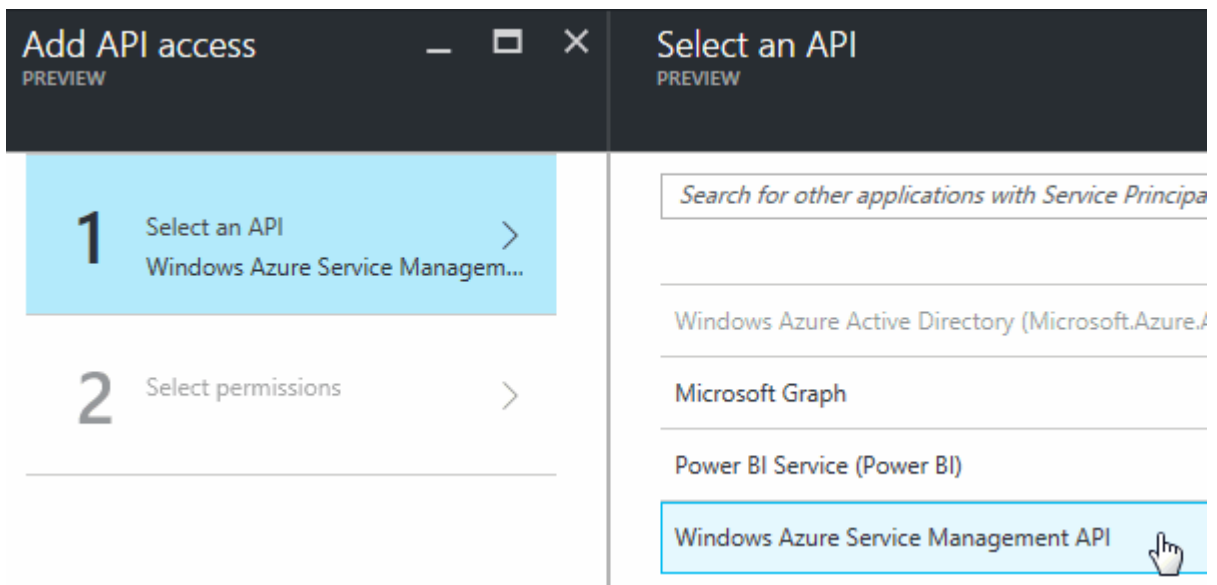


2. En el menú, haga clic en **registros de aplicaciones (Legacy)**.
3. Crear el principal de servicio:
  - a. Haga clic en **Nuevo registro de aplicación**.
  - b. Introduzca un nombre para la aplicación, mantenga seleccionada **aplicación web / API** y, a continuación, introduzca cualquier URL, por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

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



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



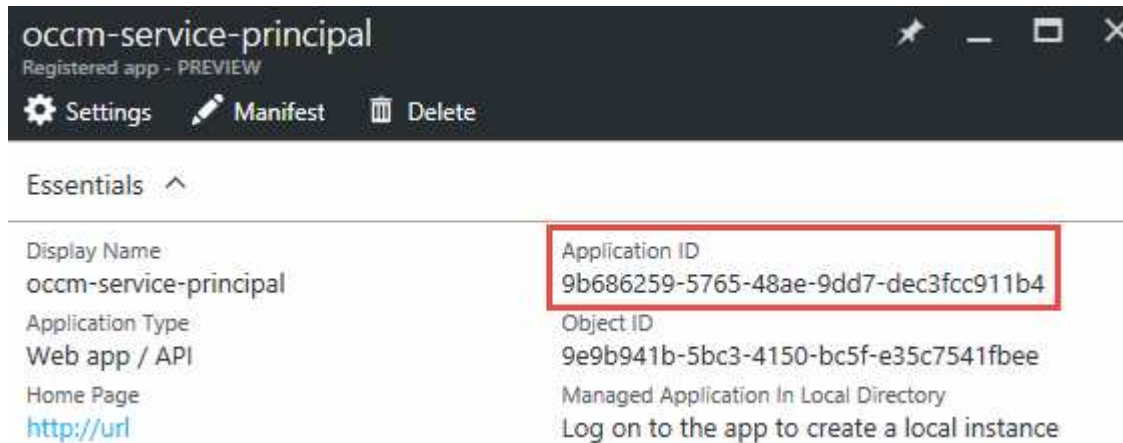
- d. Haga clic en **Access Azure Service Management as organization users**, haga clic en **Select** y, a continuación, haga clic en **Done**.
5. Cree una clave para el principal de servicio:
- En Configuración, haga clic en **teclas**.
  - Introduzca una descripción, seleccione una duración y, a continuación, haga clic en **Guardar**.
  - Copie el valor clave.

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



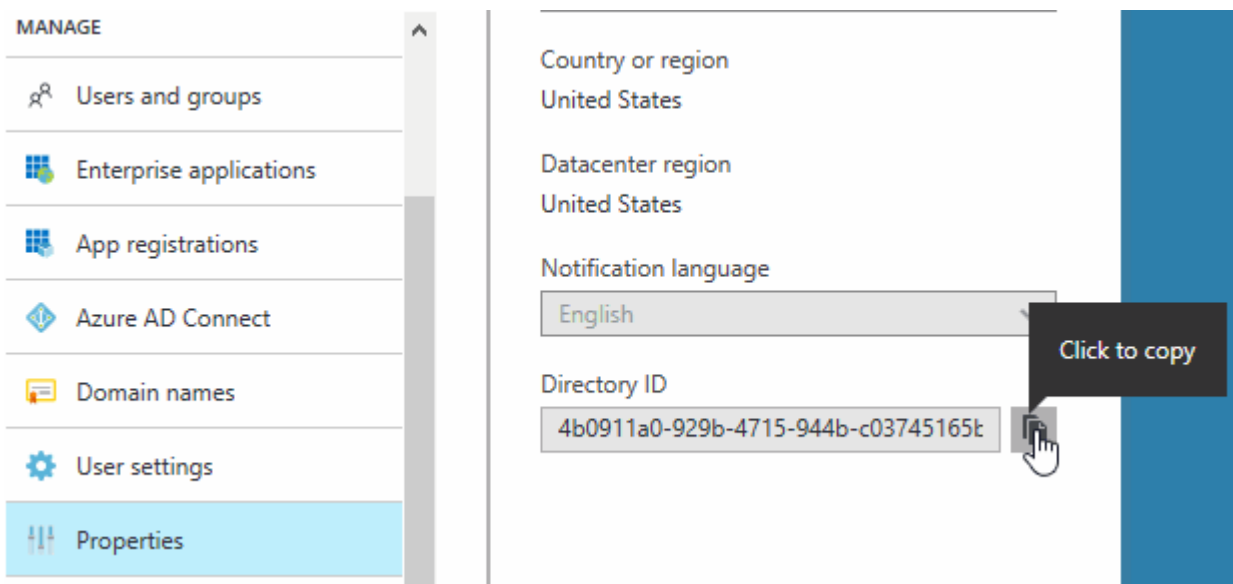
d. Haga clic en **Propiedades** y, a continuación, copie el ID de la aplicación para el principal de servicio.

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



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

- En el menú Active Directory, haga clic en **Propiedades**.
- Copie el ID del directorio.



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

## Resultado

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

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

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

### Acerca de esta tarea

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

### Pasos

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

### Resultado

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

### Adición de cuentas de Azure a Cloud Manager

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

### Pasos

1. En la parte superior derecha de la consola de Cloud Manager, haga clic en la lista desplegable de tareas y, a continuación, seleccione **Configuración de cuenta**.
2. Haga clic en **Agregar nueva cuenta** y seleccione **Microsoft Azure**.
3. Introduzca la información acerca del director del servicio de Azure Active Directory que otorga los permisos necesarios.
4. Confirme que se han cumplido los requisitos de la directiva y, a continuación, haga clic en **Crear cuenta**.

### Resultado

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



## Microsoft Azure Provider Account

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 inicial "cuenta del proveedor de cloud" Cuando pone en marcha Cloud Manager desde NetApp Cloud Central. Cuando implementó Cloud Manager, Cloud Central creó la función del operador de Cloud Manager de OnCommand y la asignó a la máquina virtual de Cloud Manager.

#### Pasos

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



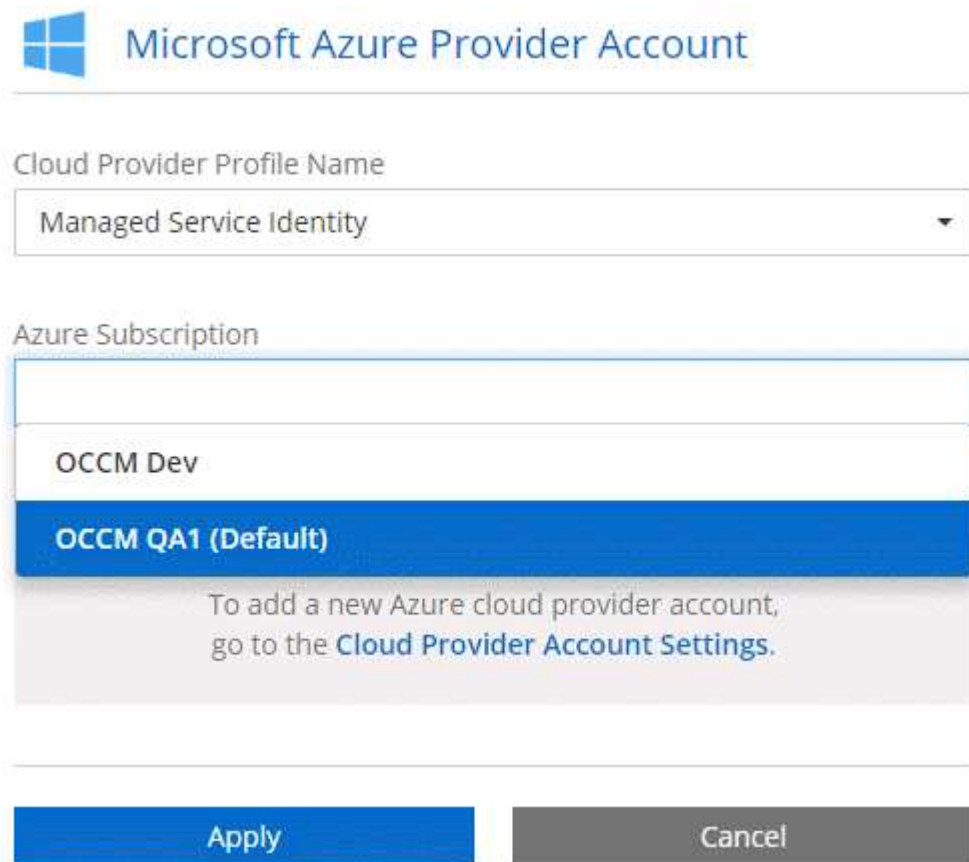
El nombre predeterminado que se proporciona en la es el operador de OnCommand Cloud Manager "Política de Cloud Manager". Si seleccionó otro nombre para el rol, seleccione ese nombre.

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

4. Repita estos pasos para suscripciones adicionales.

### Resultado

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



Microsoft Azure Provider Account

Cloud Provider Profile Name

Managed Service Identity

Azure Subscription

OCCM Dev

**OCCM QA1 (Default)**

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

Apply Cancel

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

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

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

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

### Pasos

1. Si aún no dispone de una cuenta en la página de soporte de NetApp, ["regístrese para uno"](#).
2. En la parte superior derecha de la consola de Cloud Manager, haga clic en la lista desplegable de tareas y, a continuación, seleccione **Configuración de cuenta**.
3. Haga clic en **Agregar nueva cuenta** y seleccione **Sitio de soporte de NetApp**.
4. Escriba un nombre para la cuenta y, a continuación, escriba el nombre de usuario y la contraseña.
  - La cuenta debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal).
  - Si tiene pensado poner en marcha sistemas BYOL:
    - La cuenta debe estar autorizada para acceder a los números de serie de los sistemas BYOL.
    - Si ha adquirido una suscripción BYOL segura, será necesaria una cuenta de NSS segura.
5. Haga clic en **Crear cuenta**.

## El futuro

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

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

## Instalar un certificado HTTPS para obtener acceso seguro

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

### Pasos

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

Opción	Descripción
Genere una CSR	<p>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>.</p> <p>Cloud Manager muestra una solicitud de firma de certificación.</p> <p>b. Utilice la CSR para enviar una solicitud de certificado SSL a una CA.</p> <p>El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.</p> <p>c. Copie el contenido del certificado firmado, péguelo en el campo Certificado y, a continuación, haga clic en <b>instalar</b>.</p>

Opción	Descripción
Instale su propio certificado firmado por CA	<p>a. Seleccione <b>instalar certificado firmado por CA</b>.</p> <p>b. Cargue el archivo de certificado y la clave privada y, a continuación, haga clic en <b>instalar</b>.</p> <p>El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.</p>

## 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

## Configurar usuarios e inquilinos

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

### Añadiendo usuarios a Cloud Manager

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

#### Pasos

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

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

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

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

#### El futuro

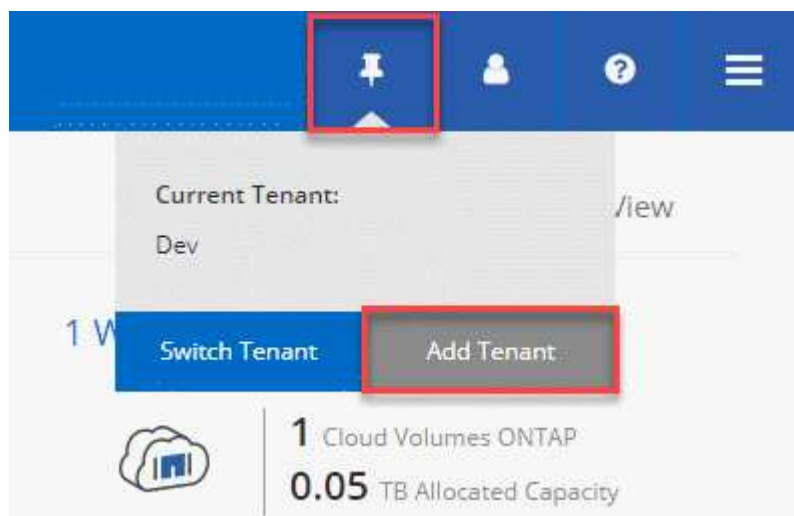
Informe al usuario de que ahora puede iniciar sesión en el sistema Cloud Manager.

## Creación de inquilinos

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

#### Pasos

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



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

#### El futuro

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

## Configuración de AWS KMS

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

#### Pasos

- 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 \(CMKs\)"](#)

- 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"

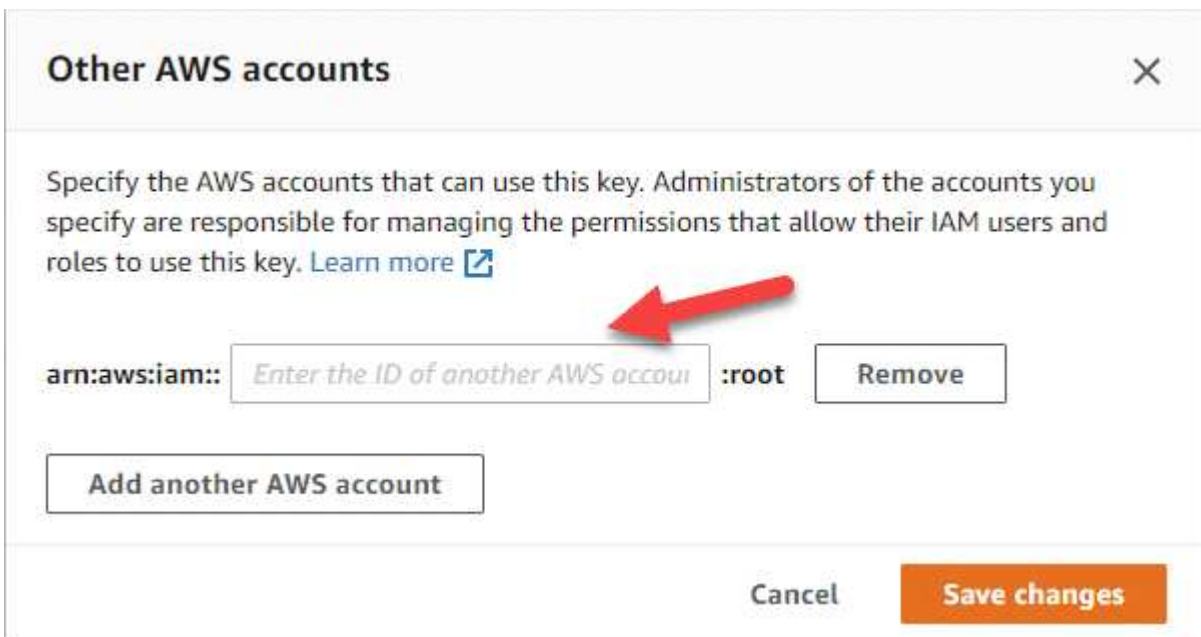
3. Si el CMK se encuentra en una cuenta de AWS diferente, realice los pasos siguientes:

- 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.