



# **Administrar BlueXP**

## **Set up and administration**

NetApp

March 13, 2023

This PDF was generated from <https://docs.netapp.com/es-es/cloud-manager-setup-admin/task-managing-netapp-accounts.html> on March 13, 2023. Always check docs.netapp.com for the latest.

# Tabla de Contenido

- Administrar BlueXP ..... 1
  - Cuentas de NetApp ..... 1
  - Conectores ..... 15
  - Gestionar suscripciones y contratos de PAYGO ..... 43
  - Almacenamiento en cloud detectado ..... 45
  - Credenciales de AWS ..... 49
  - Credenciales de Azure ..... 58
  - Credenciales de Google Cloud ..... 71
  - Gestione cuentas del sitio de soporte de NetApp en BlueXP ..... 77
  - Mis oportunidades ..... 85

# Administrar BlueXP

## Cuentas de NetApp

### Gestione su cuenta de NetApp

"[Después de realizar la configuración inicial](#)", Puede administrar la configuración de su cuenta posteriormente mediante la administración de usuarios, cuentas de servicio, áreas de trabajo y conectores.

"[Obtenga más información sobre el funcionamiento de las cuentas de NetApp](#)".

### Gestiona tu cuenta con la API de tenancy

Si desea administrar la configuración de su cuenta enviando solicitudes de API, deberá utilizar la API *Tenancy*. Esta API es diferente de la API de BlueXP, que se utiliza para crear y gestionar entornos de trabajo de Cloud Volumes ONTAP.

"[Vea los extremos de la API de tenancy](#)"

### Crear y administrar usuarios

Los usuarios de su cuenta pueden acceder a la gestión de los recursos en los espacios de trabajo de su cuenta.

#### Adición de usuarios

Asocie los usuarios con su cuenta de NetApp para que esos usuarios puedan crear y gestionar entornos de trabajo en BlueXP.

#### Pasos

1. Si el usuario aún no lo ha hecho, pida al usuario que vaya a. "[Sitio web de NetApp BlueXP](#)" y regístrese.
2. En la parte superior de BlueXP, haga clic en el menú desplegable **cuenta**.



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



4. En la ficha Miembros, haga clic en **Usuario asociado**.
5. Introduzca la dirección de correo electrónico del usuario y seleccione un rol para el usuario:
  - **Administración de cuentas:** Puede realizar cualquier acción en BlueXP.
  - **Administración de área de trabajo:** Puede crear y administrar recursos en áreas de trabajo asignadas.
  - **Visor de cumplimiento:** Sólo puede ver la información de cumplimiento de Cloud Data Sense y generar informes para áreas de trabajo a las que tienen permiso de acceso.
  - **SnapCenter Admin:** Puede utilizar el servicio SnapCenter para crear copias de seguridad coherentes con la aplicación y restaurar datos utilizando dichas copias de seguridad. *Este servicio está actualmente en Beta.*
6. Si ha seleccionado Administrador de área de trabajo o Visor de cumplimiento, seleccione uno o varios espacios de trabajo para asociarlos con ese usuario.



The image shows a dialog box titled "Associate User" with a user icon at the top. It contains instructions on how to add a user, followed by three input fields: "User's Email" (containing "test@netapp.com"), "Role" (a dropdown menu showing "Workspace Admin"), and "Associate User to Workspaces" (a dropdown menu showing "Workspace-1" with a close button). At the bottom are "Cancel" and "Associate User" buttons.



### 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

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

7. Haga clic en **asociar**.

#### Resultado

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

#### Quitar usuarios

Desasociar un usuario hace que pueda dejar de acceder a los recursos de una cuenta de NetApp.

#### Pasos

1. En la parte superior de BlueXP, haga clic en el menú desplegable **cuenta** y haga clic en **Administrar cuenta**.



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



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

## Resultado

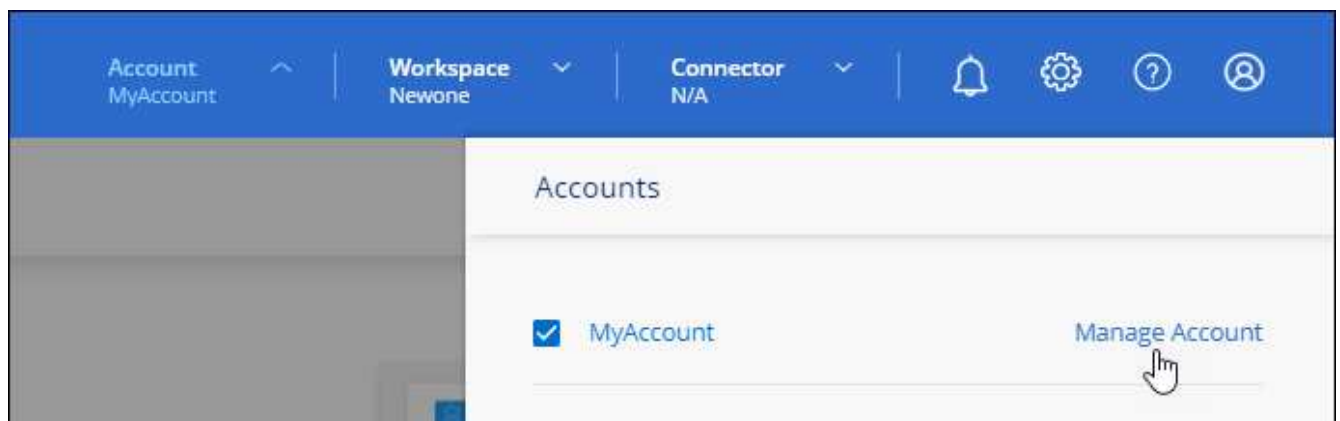
El usuario ya no puede acceder a los recursos de esta cuenta de NetApp.

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

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

## Pasos

1. En la parte superior de BlueXP, haga clic en el menú desplegable **cuenta** y haga clic en **Administrar cuenta**.



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

5 Members						
Type	Name	Email	Role	Workspace		
	Ben		☆ Account Admin	All Workspaces	...	
	Tom		☆ Account Admin	All Workspaces	...	
	Ben		Workspace Admin	Newone		

3. Haga clic en **Administrar espacios de trabajo**.

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

## Resultado

Ahora el usuario puede acceder a esas áreas de trabajo desde BlueXP, siempre y cuando el conector también esté asociado a las áreas de trabajo.

## Crear y administrar cuentas de servicio

Una cuenta de servicio actúa como un "usuario" que puede realizar llamadas API autorizadas a BlueXP con fines de automatización. Esto facilita la gestión de la automatización, ya que no necesita crear scripts de automatización basados en la cuenta de usuario de una persona real que pueda salir de la empresa en cualquier momento. Y si utiliza federation, puede crear un token sin que genere un token de actualización desde el cloud.

Usted otorga permisos a una cuenta de servicio asignándole una función, al igual que cualquier otro usuario de BlueXP. También puede asociar la cuenta de servicio a espacios de trabajo específicos para controlar los entornos de trabajo (recursos) a los que puede acceder el servicio.

Al crear la cuenta de servicio, BlueXP permite copiar o descargar un ID de cliente y un secreto de cliente para la cuenta de servicio. Este par de claves se utiliza para la autenticación con BlueXP.

### Crear una cuenta de servicio

Cree tantas cuentas de servicio como necesite para gestionar los recursos en sus entornos de trabajo.

## Pasos

1. En la parte superior de BlueXP, haga clic en el menú desplegable **cuenta**.



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



3. En la ficha Miembros, haga clic en **Crear cuenta de servicio**.
4. Introduzca un nombre y seleccione un rol. Si ha elegido una función que no sea Administrador de cuentas, elija el área de trabajo para asociarla con esta cuenta de servicio.
5. Haga clic en **Crear**.
6. Copie o descargue el ID del cliente y el secreto del cliente.

El secreto de cliente sólo es visible una vez y BlueXP no lo almacena en ninguna parte. Copie o descargue el secreto y guárdelo de forma segura.

7. Haga clic en **Cerrar**.

#### Obtención de un token de portador para una cuenta de servicio

Para realizar llamadas API al "[API de tenancy](#)", necesitará obtener un token del portador para una cuenta de servicio.

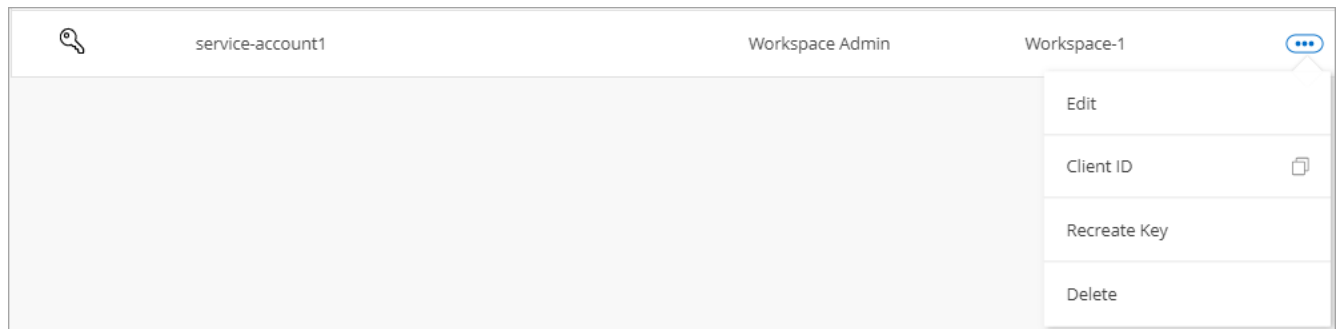
["Aprenda a crear un token de cuenta de servicio"](#)

#### Copiando el ID de cliente

Puede copiar el ID de cliente de una cuenta de servicio en cualquier momento.

#### Pasos

1. En la ficha Miembros , haga clic en el menú de acciones de la fila correspondiente a la cuenta de servicio.



2. Haga clic en **ID de cliente**.
3. El ID se copia en el portapapeles.

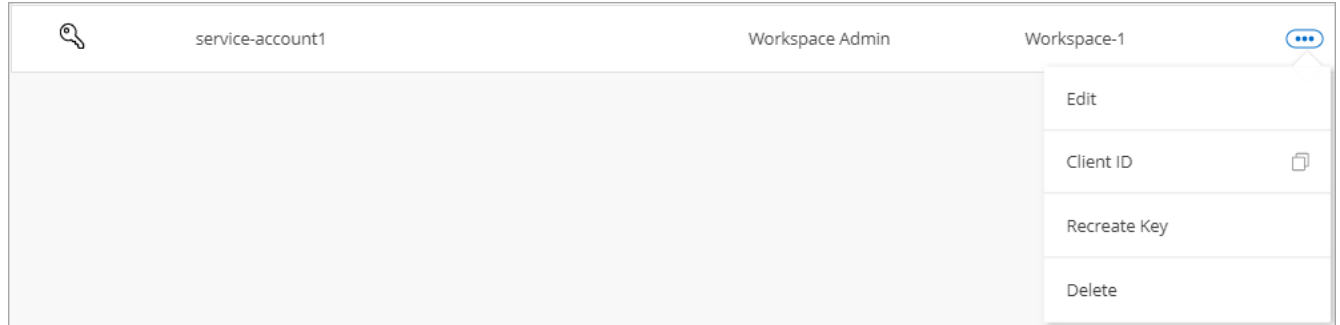


## Recrear claves

Al volver a crear la clave se eliminará la clave existente para esta cuenta de servicio y, a continuación, se creará una clave nueva. No podrá utilizar la clave anterior.

### Pasos

1. En la ficha Miembros , haga clic en el menú de acciones de la fila correspondiente a la cuenta de servicio.



2. Haga clic en **Volver a crear clave**.
3. Haga clic en **Volver a crear** para confirmar.
4. Copie o descargue el ID del cliente y el secreto del cliente.

El secreto de cliente sólo es visible una vez y BlueXP no lo almacena en ninguna parte. Copie o descargue el secreto y guárdelo de forma segura.

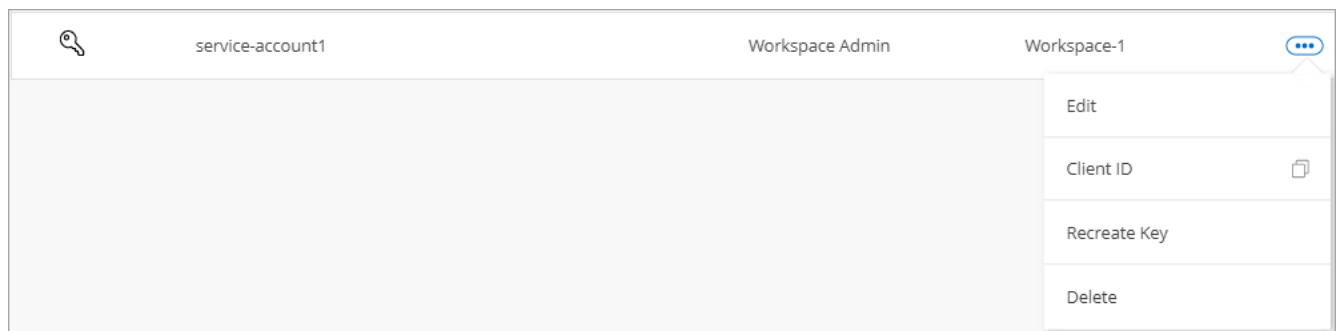
5. Haga clic en **Cerrar**.

## Eliminación de una cuenta de servicio

Elimine una cuenta de servicio si ya no necesita utilizarla.

### Pasos

1. En la ficha Miembros , haga clic en el menú de acciones de la fila correspondiente a la cuenta de servicio.



2. Haga clic en **Eliminar**.
3. Vuelva a hacer clic en **Eliminar** para confirmar.

## Gestión de espacios de trabajo

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

## Pasos

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

## Gestión de los espacios de trabajo de un conector

Debe asociar el conector con áreas de trabajo para que los administradores de área de trabajo puedan acceder a esas áreas de trabajo desde BlueXP.

Si sólo tiene Administradores de cuentas, no es necesario asociar el conector a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todas las áreas de trabajo de BlueXP de forma predeterminada.

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

## Pasos

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

## Cambio del nombre de cuenta

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

## Pasos

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

## Permitir vistas previas privadas

Permita una vista previa privada de su cuenta para obtener acceso a los nuevos servicios cloud de NetApp que están disponibles como vista previa en BlueXP.

No se garantiza que los servicios de la vista previa privada se comporten como se espera y podrían soportar interrupciones de servicio y que falten funciones.

## Pasos

1. En la parte superior de BlueXP, haga clic en el menú desplegable **cuenta** y haga clic en **Administrar cuenta**.

2. En la ficha **Descripción general**, active la opción **permitir vista previa privada**.

### Permitir servicios de terceros

Permita que los servicios de terceros de su cuenta tengan acceso a servicios de terceros disponibles en BlueXP. Los servicios de terceros son servicios de cloud similares a los que ofrece NetApp, pero son gestionados y respaldados por empresas terceros.

#### Pasos

1. En la parte superior de BlueXP, haga clic en el menú desplegable **cuenta** y haga clic en **Administrar cuenta**.
2. En la ficha **Descripción general**, active la opción **permitir servicios de terceros**.

### Supervisar operaciones en su cuenta


Puede supervisar el estado de las operaciones que está realizando BlueXP para ver si hay algún problema que necesite solucionar. Puede ver el estado en el Centro de notificaciones, en la línea de tiempo o enviar notificaciones al correo electrónico.

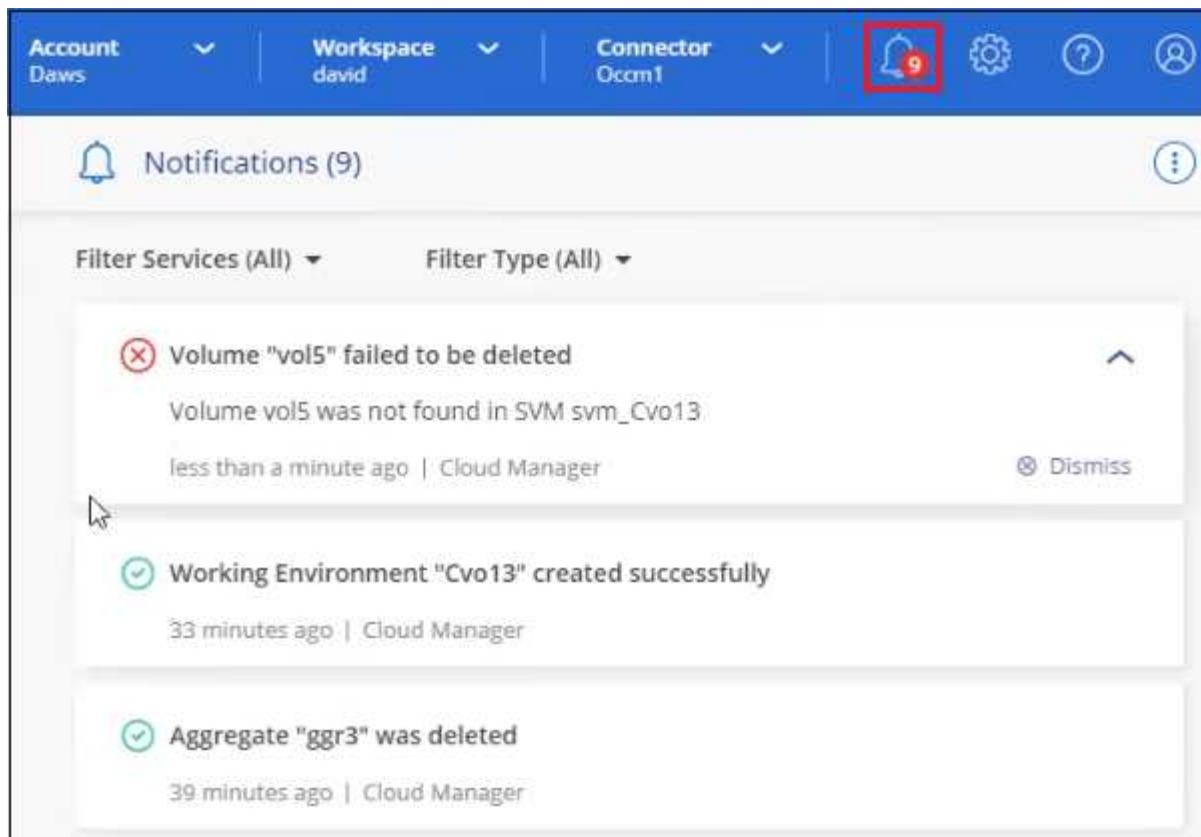
Esta tabla proporciona una comparación entre el Centro de notificación y la línea de tiempo para que pueda entender lo que cada uno puede ofrecer.

Centro de notificaciones	Línea de tiempo
Muestra el estado de alto nivel de eventos y acciones	Proporciona detalles sobre cada evento o acción para una investigación posterior
Muestra el estado de la sesión de inicio de sesión actual: La información no aparecerá en el Centro de notificaciones después de cerrar la sesión	Conserva el estado del último mes
Muestra solo las acciones iniciadas en la interfaz de usuario	Muestra todas las acciones de la interfaz de usuario o las API
Muestra acciones iniciadas por el usuario	Muestra todas las acciones, ya sean iniciadas por el usuario o iniciadas por el sistema
Filtrar resultados por importancia	Filtrar por servicio, acción, usuario, estado, etc.
Permite enviar notificaciones por correo electrónico a los usuarios de la cuenta y a otros usuarios	No dispone de funciones de correo electrónico

### Supervisión de las actividades mediante el Centro de notificación

Las notificaciones realizan un seguimiento del progreso de las operaciones que ha iniciado en BlueXP para que pueda comprobar si la operación se ha realizado correctamente o no. Le permiten ver el estado de muchas acciones de BlueXP que inició durante su sesión de inicio de sesión actual. No todos los servicios informan la información en el Centro de notificación en este momento.

Puede mostrar las notificaciones haciendo clic en la campana de notificación () en la barra de menús. El color de la pequeña burbuja en la campana indica la notificación de gravedad de nivel más alto que está activa. Así que si ves una burbuja roja, significa que hay una notificación importante que debes mirar.



También puede configurar BlueXP para que envíe notificaciones por correo electrónico de modo que pueda ser informado de la actividad importante del sistema incluso cuando no haya iniciado sesión en el sistema. Los correos electrónicos pueden enviarse a usuarios que forman parte de su cuenta de cloud de NetApp o a cualquier otro destinatario que deba conocer ciertos tipos de actividad del sistema. Consulte [Configuración de los ajustes de notificación por correo electrónico](#) a continuación.

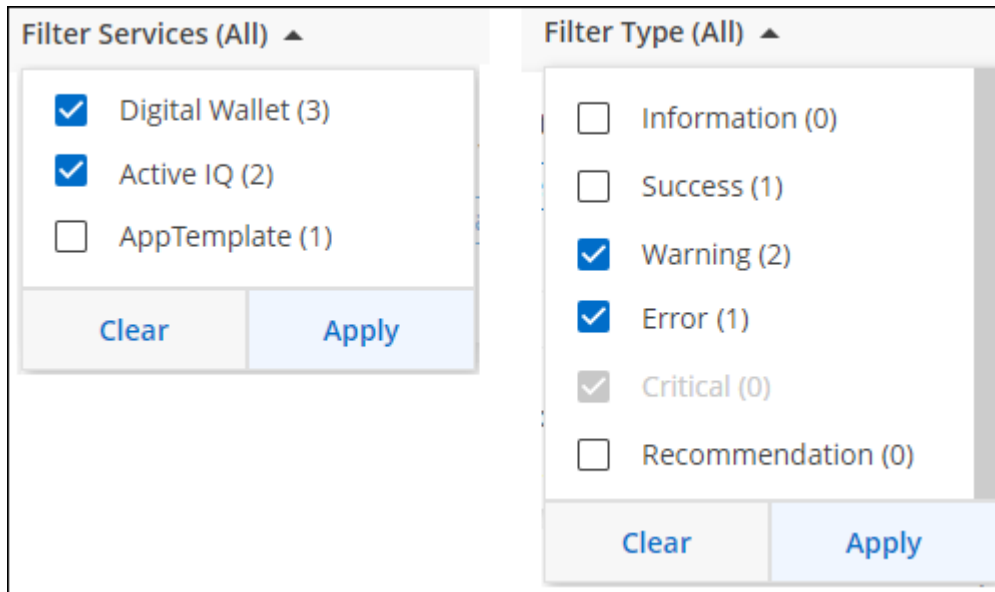
### Tipos de notificación

Las notificaciones se clasifican en las siguientes categorías:

Tipo de notificación	Descripción
Crítico	Se produjo un problema que podría provocar una interrupción del servicio si no se toman acciones correctivas de inmediato.
Error	Una acción o proceso terminado con un fallo, o podría dar lugar a un fallo si no se toma una acción correctiva.
Advertencia	Un problema que debe tener en cuenta para asegurarse de que no alcanza la gravedad crucial. Las notificaciones de esta gravedad no provocan interrupciones en el servicio y es posible que no sea necesario realizar ninguna acción correctiva al instante.
Recomendación	Una recomendación del sistema para que usted tome una acción para mejorar el sistema o un servicio determinado; por ejemplo: Ahorro de costos, sugerencia para nuevos servicios, configuración de seguridad recomendada, etc.
Información	Mensaje que proporciona información adicional sobre una acción o proceso.
Correcto	Una acción o proceso completado correctamente.

## Filtrado de notificaciones

De forma predeterminada, verá todas las notificaciones. Puede filtrar las notificaciones que aparecen en el Centro de notificaciones para que aparezcan únicamente las notificaciones que sean importantes para usted. Puede filtrar por "Servicio" de BlueXP y por "Tipo" de notificación.



The screenshot shows two side-by-side filter panels. The left panel, titled 'Filter Services (All)', contains three items: 'Digital Wallet (3)' with a checked checkbox, 'Active IQ (2)' with a checked checkbox, and 'AppTemplate (1)' with an unchecked checkbox. Below these items are two buttons: 'Clear' and 'Apply'. The right panel, titled 'Filter Type (All)', contains six items: 'Information (0)' with an unchecked checkbox, 'Success (1)' with an unchecked checkbox, 'Warning (2)' with a checked checkbox, 'Error (1)' with a checked checkbox, 'Critical (0)' with a checked checkbox, and 'Recommendation (0)' with an unchecked checkbox. Below these items are two buttons: 'Clear' and 'Apply'.

Por ejemplo, si desea ver sólo las notificaciones "error" y "Advertencia" para las operaciones de BlueXP, seleccione esas entradas y sólo verá esos tipos de notificaciones.

## Configuración de los ajustes de notificación por correo electrónico

Puede enviar tipos específicos de notificaciones por correo electrónico para que se le informe de la actividad importante del sistema incluso cuando no haya iniciado sesión en BlueXP. Los correos electrónicos pueden enviarse a usuarios que formen parte de su cuenta de NetApp o a cualquier otro destinatario que deba conocer ciertos tipos de actividad del sistema.



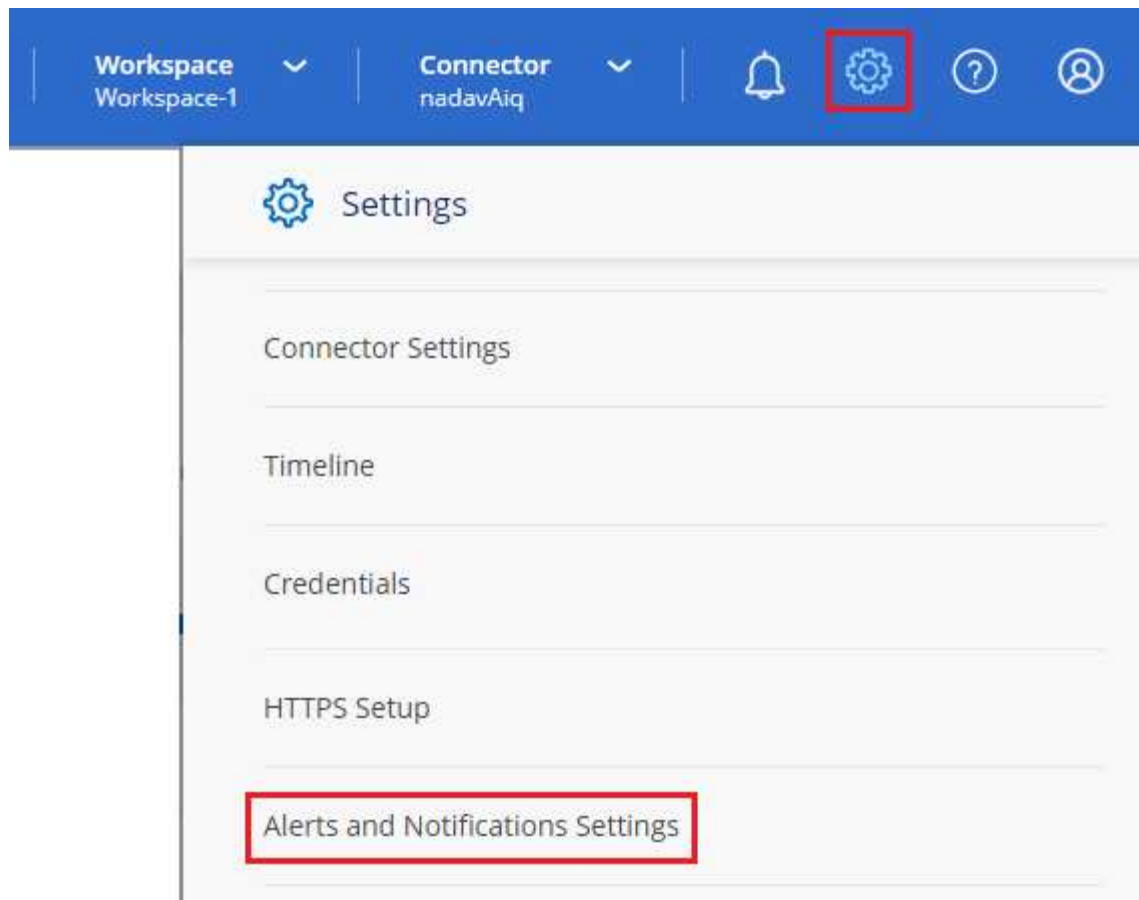
- En este momento, se envían notificaciones por correo electrónico para las siguientes características y servicios de BlueXP: Conectores, Cloud Sync, Cloud Backup y Protección contra ransomware. En futuras versiones se añadirán servicios adicionales.
- No se admite el envío de notificaciones por correo electrónico cuando el conector está instalado en un sitio sin acceso a Internet.

De forma predeterminada, los administradores de cuentas de BlueXP recibirán correos electrónicos para todas las notificaciones "críticas" y "recomendaciones". Todos los demás usuarios y destinatarios están configurados, de forma predeterminada, para no recibir ningún correo electrónico de notificación.

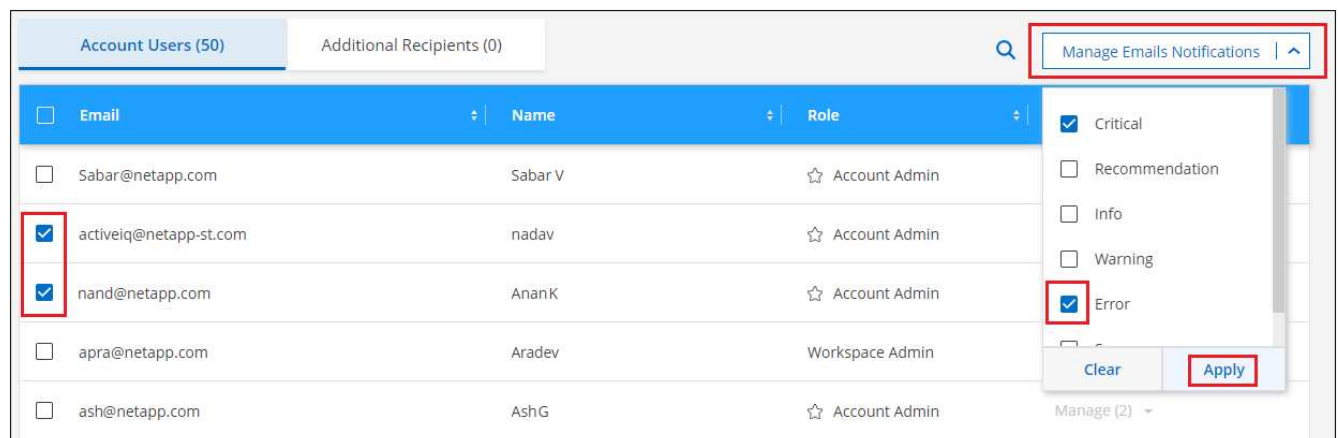
Debe ser un administrador de cuentas para personalizar los ajustes de notificaciones.

## Pasos

1. En la barra de menús de BlueXP, haga clic en **Configuración > Configuración de alertas y notificaciones**.



2. Seleccione un usuario o varios usuarios en la ficha *Account Users* o en la ficha *Additional Recipients* y elija el tipo de notificaciones que desea enviar:
  - Para realizar cambios para un único usuario, haga clic en el menú de la columna Notificaciones de ese usuario, compruebe los tipos de notificaciones que se van a enviar y haga clic en **aplicar**.
  - Para realizar cambios en varios usuarios, active la casilla de cada usuario, haga clic en **Administrar notificaciones por correo electrónico**, seleccione los tipos de notificaciones que desea enviar y haga clic en **aplicar**.



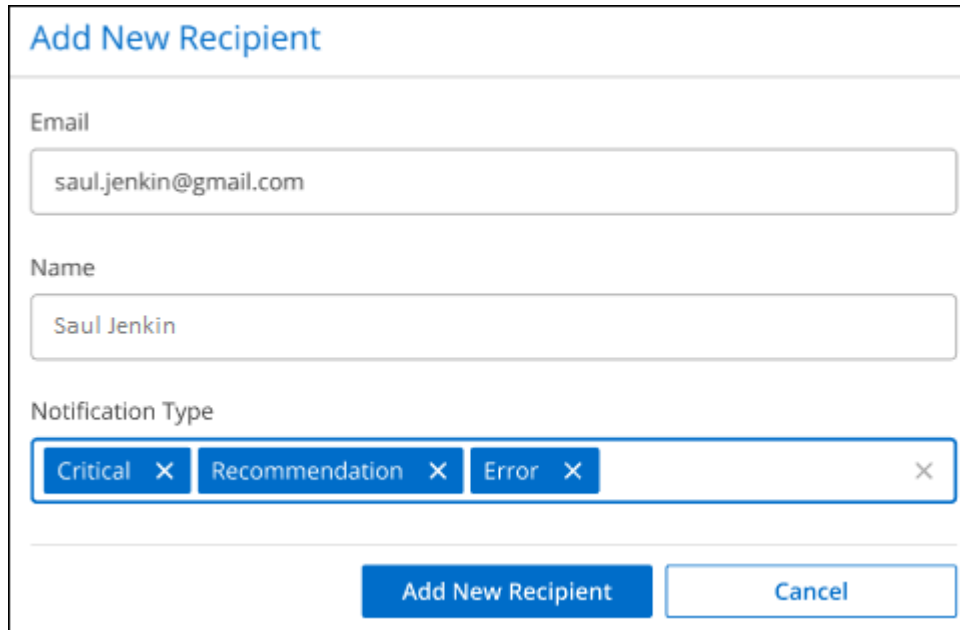
#### Adición de destinatarios de correo electrónico adicionales

Los usuarios que aparecen en la pestaña *Account Users* se rellenan automáticamente desde los usuarios de su cuenta de NetApp (en la "[Gestionar cuenta](#)"). Puede agregar direcciones de correo electrónico en la ficha

*Additional Recipients* para otras personas o grupos que no tienen acceso a BlueXP, pero que necesitan recibir notificaciones sobre ciertos tipos de alertas y notificaciones.

## Pasos

1. En la página Configuración de alertas y notificaciones, haga clic en **Agregar nuevos destinatarios**.



2. Introduzca el nombre y la dirección de correo electrónico, seleccione los tipos de notificaciones que recibirá el destinatario y haga clic en **Agregar nuevo destinatario**.

## Notificaciones faltantes

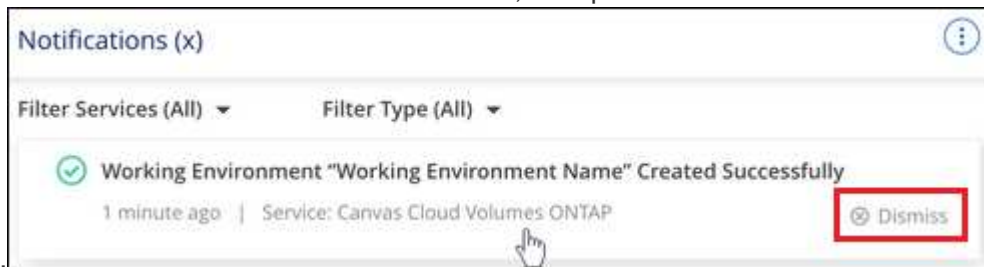
Puede eliminar notificaciones de la página si ya no necesita verlos. Puede descartar todas las notificaciones al mismo tiempo o descartar notificaciones individuales.

Para descartar todas las notificaciones, en el Centro de notificaciones, haga clic en  Y selecciona **descartar**



todo.

Para descartar notificaciones individuales, coloque el cursor sobre la notificación y haga clic en **descartar**



## Auditar la actividad de usuario en su cuenta

La línea de tiempo de BlueXP muestra las acciones que los usuarios han completado para administrar su cuenta. Esto incluye acciones de gestión como asociar usuarios, crear áreas de trabajo, crear conectores y mucho más.

La comprobación de la línea de tiempo puede ser útil si necesita identificar quién realizó una acción específica o si necesita identificar el estado de una acción.

## Pasos

1. En la barra de menús de BlueXP, haga clic en **Configuración > línea de tiempo**.
2. En los filtros, haga clic en **Servicio**, active **Cliente** y haga clic en **aplicar**.

## Resultado

La línea de tiempo se actualiza para mostrar las acciones de gestión de cuentas.

## Funciones

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

El rol Compliance Viewer es para acceso de sólo lectura a Cloud Data Sense.

Tarea	Administrador de cuentas	Administrador de área de trabajo	Visor de cumplimiento de normativas	Administrador de SnapCenter
Gestionar entornos de trabajo	Sí	Sí	No	No
Activar servicios en entornos de trabajo	Sí	Sí	No	No
Ver el estado de replicación de datos	Sí	Sí	No	No
Visualice la línea de tiempo	Sí	Sí	No	No
Cambiar entre espacios de trabajo	Sí	Sí	Sí	No
Ver resultados de análisis de detección de datos	Sí	Sí	Sí	No
Eliminar entornos de trabajo	Sí	No	No	No
Conecte los clústeres de Kubernetes a entornos de trabajo	Sí	No	No	No
Reciba el informe de Cloud Volumes ONTAP	Sí	No	No	No
Crear conectores	Sí	No	No	No
Gestione cuentas de NetApp	Sí	No	No	No
Gestionar credenciales	Sí	No	No	No



Tarea	Administrador de cuentas	Administrador de área de trabajo	Visor de cumplimiento de normativas	Administrador de SnapCenter
Modificar la configuración de BlueXP	Sí	No	No	No
Consulte y gestione la consola de soporte	Sí	No	No	No
Eliminar entornos de trabajo de BlueXP	Sí	No	No	No
Instale un certificado HTTPS	Sí	No	No	No
Utilice el servicio SnapCenter	Sí	Sí	No	Sí

#### Enlaces relacionados

- ["Configuración de espacios de trabajo y usuarios en la cuenta de NetApp"](#)
- ["Gestión de espacios de trabajo y usuarios en la cuenta de NetApp"](#)

## Conectores

### Puesta en marcha avanzada

#### Cree un conector desde AWS Marketplace

Para una región comercial de AWS, lo mejor es crear un conector directamente desde BlueXP, pero puede ejecutar un conector desde AWS Marketplace, si lo prefiere. Para regiones gubernamentales de AWS, no es posible poner en marcha el conector en una región gubernamental desde el sitio web BlueXP SaaS, por lo que la mejor opción es hacerlo desde AWS Marketplace.



También puede descargar e instalar el software Connector en un host Linux existente en su red o en la nube. ["Aprenda a instalar el conector en un host Linux existente"](#).

#### Cree el conector en una región comercial de AWS

Puede iniciar la instancia de Connector en una región comercial de AWS directamente desde la oferta de AWS Marketplace para BlueXP.

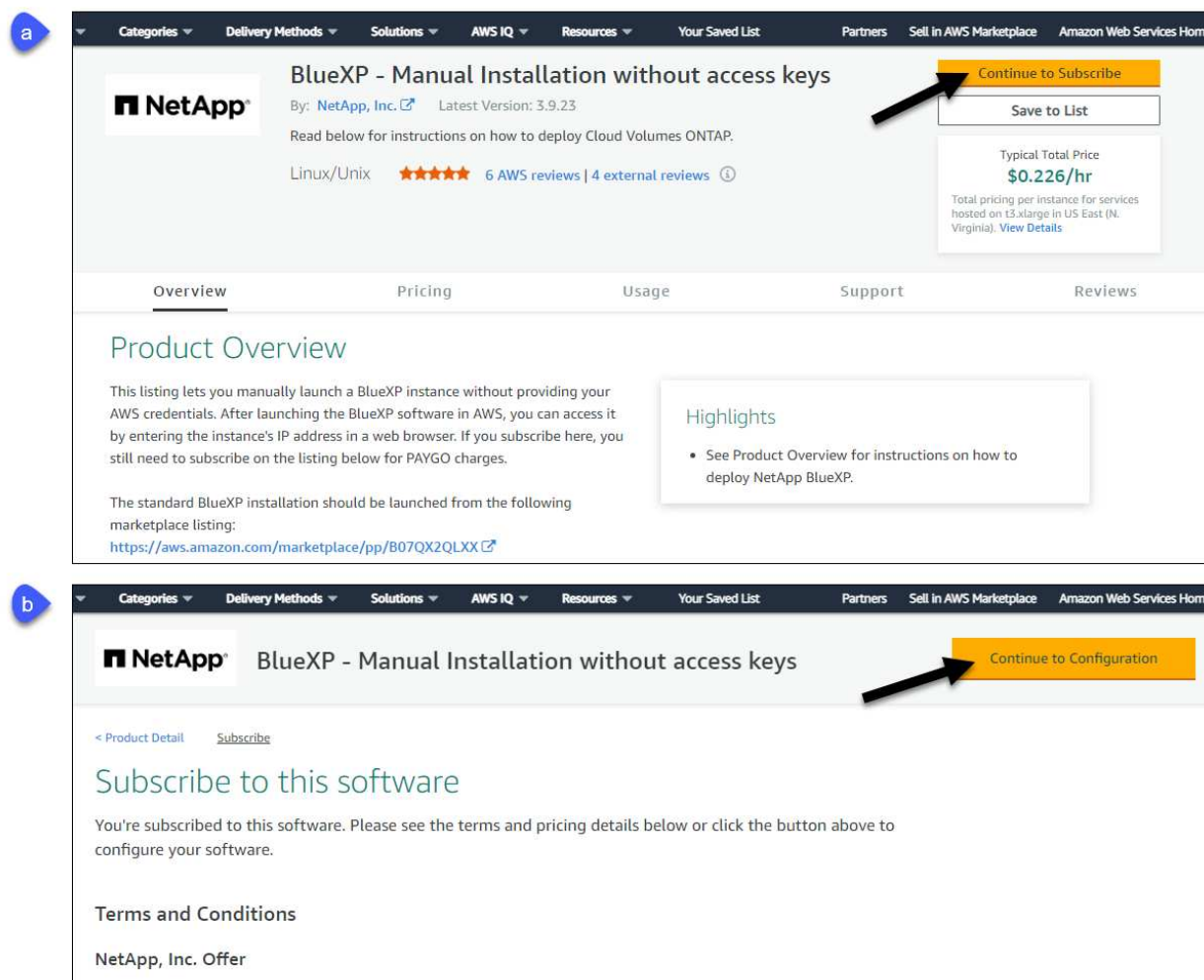
#### Antes de empezar

El usuario de IAM que crea el conector debe tener permisos de AWS Marketplace para suscribirse y cancelar su suscripción.

#### Pasos

1. Configure permisos en AWS:
  - a. Desde la consola IAM, cree las directivas necesarias copiando y pegando el contenido de ["Políticas de IAM para el conector"](#).

- b. Cree un rol IAM con el tipo de rol Amazon EC2 y adjunte las políticas que creó en el paso anterior al rol.
2. Vaya a la "[Página de BlueXP en AWS Marketplace](#)" Para desplegar el conector desde un AMI:
3. En la página Marketplace, haga clic en **continuar a Suscribirse** y luego haga clic en **continuar a Configuración**.



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

Estos pasos describen cómo iniciar la instancia desde la consola EC2 porque la consola permite asociar una función IAM a la instancia del conector. Esto no es posible usando la acción **Iniciar desde el sitio web**.

6. Siga las instrucciones para configurar y desplegar la instancia:
  - **Nombre y etiquetas:** Introduzca un nombre y etiquetas para la instancia.
  - **Aplicación y OS Image:** Omitir esta sección. El conector AMI ya está seleccionado.
  - **Tipo de instancia:** En función de la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.xlarge).

"[Revise los requisitos de la instancia](#)".

- **Par de claves (login):** Seleccione el par de claves que desea utilizar para conectarse de forma segura a la instancia.
- **Ajustes de red:** Edite los ajustes de red según sea necesario:
  - Elija el VPC y la subred que desee.
  - Especifique si la instancia debe tener una dirección IP pública.
  - Especifique la configuración del firewall que habilite los métodos de conexión necesarios para la instancia del conector: SSH, HTTP y HTTPS.
- **Configurar almacenamiento:** Mantenga las opciones de almacenamiento predeterminadas.
- **Detalles avanzados:** En **perfil de instancia de IAM**, elija la función de IAM que creó en el paso 1.
- **Resumen:** Revise el resumen y haga clic en **Iniciar instancia**.

AWS inicia el software con la configuración especificada. La instancia y el software del conector deben estar funcionando en aproximadamente cinco minutos.

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

`https://ipaddress[]`

8. Después de iniciar sesión, configure el conector:

- a. Especifique la cuenta de NetApp que desea asociar al conector.

["Obtenga más información acerca de las cuentas de NetApp"](#).

- b. Escriba un nombre para el sistema.

9. Abra un explorador web y vaya a <https://console.blueexp.netapp.com> Para empezar a utilizar el conector con BlueXP.

## Resultado

El conector ahora está instalado y configurado con su cuenta de NetApp. BlueXP utilizará este conector automáticamente cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará ["alterne entre ellos"](#).

Si tiene cubos Amazon S3 en la misma cuenta AWS en la que creó el conector, verá que aparecerá un entorno de trabajo Amazon S3 en el lienzo automáticamente. ["Obtenga más información sobre lo que puede hacer con este entorno de trabajo"](#).

## Cree el conector en una región gubernamental de AWS

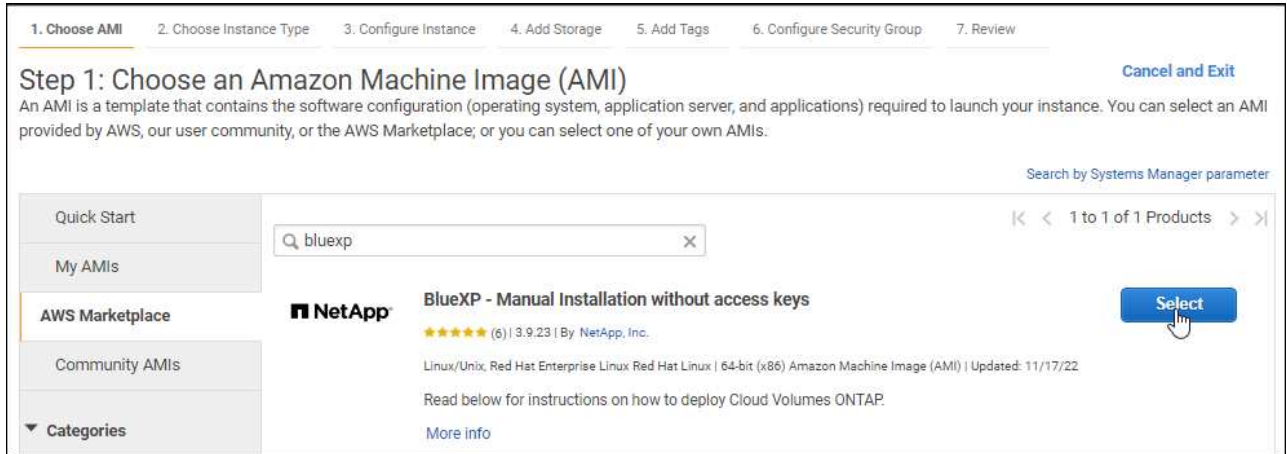
Para poner en marcha Connector en una región AWS Government, debe ir al servicio EC2 y seleccionar la oferta BlueXP en AWS Marketplace.

## Pasos

1. Configure permisos en AWS:
  - a. Desde la consola IAM, cree su propia directiva copiando y pegando el contenido de ["Política de IAM para el conector"](#).
  - b. Cree un rol IAM con el tipo de rol Amazon EC2 y asocie la política que ha creado en el paso anterior al rol.
2. Vaya a la oferta de BlueXP en AWS Marketplace.

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

- a. Abra el servicio EC2 y seleccione **Iniciar instancia**.
- b. Seleccione **AWS Marketplace**.
- c. Busque BlueXP y seleccione la oferta.



- d. Haga clic en **continuar**.

3. Siga las instrucciones para configurar y desplegar la instancia:

- **Elija un tipo de instancia:** En función de la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.xlarge).

"Revise los requisitos de la instancia".

- **Configurar detalles de instancia:** Seleccione un VPC y una subred, elija la función de IAM que creó en el paso 1, habilite la protección de terminación (recomendado) y elija cualquier otra opción de configuración que cumpla sus requisitos.

Number of instances	1	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2   VPC4QA (default)	<a href="#">Create new VPC</a>
Subnet	subnet-39536c13   QASubnet1   us-east-1b 155 IP Addresses available	<a href="#">Create new subnet</a>
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<a href="#">Create new Capacity Reservation</a>
IAM role	Cloud_Manager	<a href="#">Create new IAM role</a>
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	

- **almacenamiento:** Mantenga las opciones de almacenamiento predeterminadas.
- **Agregar etiquetas:** Introduzca etiquetas para la instancia, si lo desea.
- **Configurar grupo de seguridad:** Especifique los métodos de conexión necesarios para la instancia de conector: SSH, HTTP y HTTPS.
- **Revisión:** Revise sus selecciones y haga clic en **Iniciar**.

AWS inicia el software con la configuración especificada. La instancia y el software del conector deben estar funcionando en aproximadamente cinco minutos.

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

`https://ipaddress[]`

- Después de iniciar sesión, configure el conector:
  - Especifique la cuenta de NetApp que desea asociar al conector.  
  
["Obtenga más información acerca de las cuentas de NetApp"](#).
  - Escriba un nombre para el sistema.

## Resultado

El conector ahora está instalado y configurado con su cuenta de NetApp.

Siempre que desee utilizar BlueXP, abra el explorador Web y conéctese a la dirección IP de la instancia de Connector: `https://ipaddress[]`

Dado que el conector se desplegó en una región gubernamental, no se puede acceder a él desde <https://console.bluexp.netapp.com>.

## Abra el puerto 3128 para los mensajes de AutoSupport

Si tiene previsto implementar sistemas Cloud Volumes ONTAP en una subred en la que no esté disponible una conexión a Internet saliente, BlueXP configura automáticamente Cloud Volumes ONTAP para que utilice el conector como servidor proxy.

El único requisito es asegurarse de que el grupo de seguridad del conector permita conexiones *entrante* a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Si utiliza el grupo de seguridad predeterminado para Cloud Volumes ONTAP, no es necesario realizar cambios en su grupo de seguridad. Pero si tiene pensado definir reglas de salida estrictas para Cloud Volumes ONTAP, también tendrá que asegurarse de que el grupo de seguridad Cloud Volumes ONTAP permita conexiones *saliente* a través del puerto 3128.

## Cree un conector desde Azure Marketplace

Para una región comercial de Azure, lo mejor es crear un conector directamente desde BlueXP, pero puede ejecutar un conector desde Azure Marketplace, si lo prefiere. Para regiones gubernamentales de Azure, no es posible poner en marcha Connector en una región gubernamental desde el sitio web BlueXP SaaS, por lo que la mejor opción es hacerlo desde Azure Marketplace.



También puede descargar e instalar el software Connector en un host Linux existente en su red o en la nube. ["Aprenda a instalar el conector en un host Linux existente"](#).

### Creación de un conector en Azure

Implemente el conector en Azure con la imagen en Azure Marketplace y después inicie sesión en el conector para especificar su cuenta de NetApp.

### Pasos

1. Vaya a la página NetApp Connector VM del Azure Marketplace.
  - ["Página de Azure Marketplace para regiones comerciales"](#)
  - ["Página de Azure Marketplace para regiones gubernamentales de Azure"](#)
2. Haga clic en **Get Now** y, a continuación, haga clic en **Continue**.
3. En el portal de Azure, haga clic en **Crear** y siga los pasos para configurar la máquina virtual.

Tenga en cuenta lo siguiente al configurar la máquina virtual:

- El conector puede tener un rendimiento óptimo tanto con discos HDD como SSD.
- Elija un tamaño de máquina virtual que cumpla los requisitos de CPU y RAM. Recomendamos DS3 v2.

["Revise los requisitos de las máquinas virtuales"](#).

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

["Obtenga más información sobre las reglas de grupo de seguridad para el conector"](#).

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

Esta configuración es importante porque una identidad administrada permite que la máquina virtual Connector se identifique a sí misma en Azure Active Directory sin proporcionar credenciales. ["Obtenga más información sobre las identidades gestionadas para recursos de Azure"](#).

4. En la página **revisar + crear**, revise las selecciones y haga clic en **Crear** para iniciar la implementación.

Azure implementa la máquina virtual con los ajustes especificados. El software de la máquina virtual y el conector debe estar funcionando en aproximadamente cinco minutos.

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

`https://ipaddress[]`

6. Después de iniciar sesión, configure el conector:

- a. Especifique la cuenta de NetApp que desea asociar al conector.

["Obtenga más información acerca de las cuentas de NetApp"](#).

- b. Escriba un nombre para el sistema.

## Resultado

El conector ahora está instalado y configurado con su cuenta de NetApp.

Si el conector está en una región comercial de Azure, abra un explorador web y vaya a.

<https://console.bluexp.netapp.com> Para empezar a utilizar el conector con BlueXP.

Si Connector se encuentra en una región gubernamental de Azure, puede utilizar BlueXP abriendo su navegador web y conectándose a la dirección IP de la instancia de Connector: `https://ipaddress[]`

Dado que el conector se desplegó en una región gubernamental, no se puede acceder a él desde <https://console.bluexp.netapp.com>.

## Concesión de permisos de Azure

Cuando implementó Connector en Azure, debería haber habilitado un ["identidad administrada asignada por el sistema"](#). Ahora debe conceder los permisos de Azure necesarios creando una función personalizada y, a continuación, asignando la función a la máquina virtual Connector para una o más suscripciones.

## Pasos

1. Crear un rol personalizado:
  - a. Copie el contenido de ["Permisos de función personalizada para el conector"](#) Y guárdelos en un archivo JSON.
  - 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.

En los pasos siguientes se describe cómo crear la función mediante Bash en Azure Cloud Shell.

- Comenzar "Shell de cloud de Azure" Y seleccione el entorno Bash.
- Cargue el archivo JSON.



- Use la interfaz de línea de comandos de Azure para crear el rol personalizado:

```
az role definition create --role-definition Connector_Policy.json
```

Ahora debe tener una función personalizada denominada operador BlueXP que puede asignar a la máquina virtual Connector.

2. Asigne el rol a la máquina virtual conector para una o más suscripciones:

- a. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar sistemas Cloud Volumes ONTAP.
- b. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
- c. En la ficha **rol**, seleccione el rol **operador BlueXP** y haga clic en **Siguiente**.



BlueXP Operator es el nombre predeterminado que se proporciona en la directiva de BlueXP. Si seleccionó otro nombre para el rol, seleccione ese nombre.

- d. En la ficha **Miembros**, realice los siguientes pasos:



- Asignar acceso a una **identidad administrada**.
- Haga clic en **Seleccionar miembros**, seleccione la suscripción en la que se creó la máquina virtual Connector, elija **máquina virtual** y, a continuación, seleccione la máquina virtual Connector.
- Haga clic en **Seleccionar**.
- Haga clic en **Siguiente**.

e. Haga clic en **revisar + asignar**.

f. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

## Resultado

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

Si dispone de almacenamiento de Azure Blob en la misma cuenta de Azure en la que creó el conector, verá que aparece un entorno de trabajo de Azure Blob en el lienzo automáticamente. ["Obtenga más información sobre lo que puede hacer con este entorno de trabajo"](#).

## Abra el puerto 3128 para los mensajes de AutoSupport

Si tiene previsto implementar sistemas Cloud Volumes ONTAP en una subred en la que no esté disponible una conexión a Internet saliente, BlueXP configura automáticamente Cloud Volumes ONTAP para que utilice el conector como servidor proxy.

El único requisito es asegurarse de que el grupo de seguridad del conector permita conexiones *entrante* a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Si utiliza el grupo de seguridad predeterminado para Cloud Volumes ONTAP, no es necesario realizar cambios en su grupo de seguridad. Pero si tiene pensado definir reglas de salida estrictas para Cloud Volumes ONTAP, también tendrá que asegurarse de que el grupo de seguridad Cloud Volumes ONTAP permita conexiones *saliente* a través del puerto 3128.

## Instale el conector en un host Linux existente que tenga acceso a Internet

La forma más común de crear un conector es directamente desde BlueXP o desde el mercado de un proveedor de la nube. Pero tiene la opción de descargar e instalar el software Connector en un host Linux existente en su red o en la nube. Estos pasos son específicos de los hosts que tienen acceso a Internet.

["Obtenga información sobre otras formas de desplegar un conector"](#).



Si desea crear un sistema Cloud Volumes ONTAP en Google Cloud, debe tener un conector que también funcione en Google Cloud. No puede utilizar un conector que se ejecute en AWS, Azure o en las instalaciones.

## Verifique los requisitos del host

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

## Se requiere un host dedicado

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

## CPU

4 núcleos o 4 vCPU

## RAM

14 GB

## Tipo de instancia de AWS EC2

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos t3.xlarge.

## Tamaño de la máquina virtual de Azure

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos DS3 v2.

## Tipo de máquina GCP

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos n2-standard-4.

El conector es compatible con Google Cloud en una instancia de máquina virtual con un sistema operativo compatible "[Características de VM blindadas](#)"

## Sistemas operativos compatibles

- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6 y 8.7

El sistema Red Hat Enterprise Linux debe estar registrado con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación del conector.

El conector es compatible con las versiones en inglés de estos sistemas operativos.

## Hipervisor

Un hipervisor de configuración básica o alojado certificado Ejecute CentOS o Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"^]

## Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

## Espacio en disco en /var

Debe haber 20 GIB de espacio disponibles

## Motor Docker

Se requiere Docker Engine versión 19.3.1 o posterior en el host antes de instalar el conector. "[Ver las instrucciones de instalación](#)"

## Acceso a Internet de salida

El instalador del conector debe acceder a las siguientes direcciones URL durante el proceso de instalación:

- <https://support.netapp.com>

- <https://mysupport.netapp.com>
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://cloudmanagerinfraprod.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net)

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

### Instale el conector

Después de verificar que tiene un host Linux compatible, puede obtener el software Connector y luego instalarlo.

### Lo que necesitará

- Privilegios de root para instalar el conector.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector. Son compatibles con HTTP y HTTPS.

Tiene la opción de configurar un servidor proxy después de la instalación, pero para hacerlo es necesario reiniciar el conector.

- Un certificado firmado por CA, si el servidor proxy utiliza HTTPS.

### Acerca de esta tarea

- La instalación instala las herramientas de línea de comandos de AWS (awscli) para habilitar los procedimientos de recuperación del soporte de NetApp.

Si recibe un mensaje que ha fallado al instalar el awscli, puede ignorar el mensaje de forma segura. El conector puede funcionar correctamente sin las herramientas.

- El instalador disponible en el sitio de soporte de NetApp puede ser una versión anterior. Después de la instalación, el conector se actualiza automáticamente si hay una nueva versión disponible.

### Pasos

1. Compruebe que docker está activado y en ejecución.

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. Si las variables del sistema `http_proxy` o `https_proxy` están establecidas en el host, elimínelas:

```
unset http_proxy
unset https_proxy
```

Si no elimina estas variables del sistema, la instalación fallará.

3. Descargue el software del conector de "[Sitio de soporte de NetApp](#)"Y, a continuación, cópielo en el host

Linux.

Debe descargar el instalador de Connector que se ha diseñado para su uso en la red o en la nube.

4. Asigne permisos para ejecutar el script.

```
chmod +x OnCommandCloudManager-V3.9.23
```

5. Ejecute el script de instalación.

```
./OnCommandCloudManager-V3.9.23 --proxy <HTTP or HTTPS proxy server>  
--cacert <path and file name of a CA-signed certificate>
```

Los parámetros `--proxy` y `--cacert` son opcionales. Si tiene un servidor proxy, deberá introducir los parámetros como se muestra. El instalador no le solicita que proporcione información sobre un proxy.

A continuación encontrará un ejemplo del comando utilizando los dos parámetros opcionales:

```
./OnCommandCloudManager-V3.9.23 --proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

`--proxy` configura el conector para que utilice un servidor proxy HTTP o HTTPS con uno de los siguientes formatos:

- `http://address:port`
- `http://username:password@address:port`
- `https://address:port`
- `https://username:password@address:port`

`--cacert` especifica un certificado firmado por CA que se utilizará para el acceso HTTPS entre el conector y el servidor proxy. Este parámetro solo es obligatorio si se especifica un servidor proxy HTTPS.

## Resultado

El conector ya está instalado. Al final de la instalación, el servicio Connector (occm) se reinicia dos veces si ha especificado un servidor proxy.

## Configure el conector

Regístrese o inicie sesión y, a continuación, configure el conector para que funcione con su cuenta.

## Pasos

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

```
https://ipaddress[]
```

*ipaddress* puede ser localhost, una dirección IP privada o una dirección IP pública, dependiendo de la configuración del host. Por ejemplo, si el conector está en la nube pública sin una dirección IP pública,

debe introducir una dirección IP privada desde un host que tenga una conexión con el host del conector.

2. Regístrese o inicie sesión.
3. Si ha instalado Connector en Google Cloud, configure una cuenta de servicio que tenga los permisos que BlueXP necesita para crear y gestionar sistemas Cloud Volumes ONTAP en proyectos.
  - a. ["Crear un rol en GCP"](#) esto incluye los permisos definidos en la ["Política de conectores para GCP"](#).
  - b. ["Cree una cuenta de servicio de GCP y aplique el rol personalizado que acaba de crear"](#).
  - c. ["Asocie esta cuenta de servicio a la máquina virtual del conector"](#).
  - d. Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, ["Conceda acceso agregando la cuenta de servicio con la función BlueXP a ese proyecto"](#). Deberá repetir este paso con cada proyecto.
4. Después de iniciar sesión, configure BlueXP:
  - a. Especifique la cuenta de NetApp que desea asociar al conector.  
  
["Obtenga más información acerca de las cuentas de NetApp"](#).
  - b. Escriba un nombre para el sistema.

## Resultado

El conector ahora está instalado y configurado con su cuenta de NetApp. BlueXP utilizará este conector automáticamente cuando cree nuevos entornos de trabajo.

## Después de terminar

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

- AWS: ["Configure una cuenta de AWS y, a continuación, agréguela a BlueXP"](#)
- Azure: ["Configure una cuenta de Azure y añádala a BlueXP"](#)
- Google Cloud: Consulte el paso 3 anterior

## Instale el conector en una ubicación sin acceso a Internet

Puede instalar el conector en una ubicación que tenga un aislamiento completo de Internet, ya sea en las instalaciones o en una región de la nube. A continuación, puede utilizar los servicios BlueXP que son compatibles con ese entorno.

### Información general en las instalaciones

En un entorno local sin Internet, puede utilizar BlueXP para detectar clústeres de ONTAP en las instalaciones, replicar datos entre ellos, realizar backups de volúmenes con Cloud Backup y analizarlos con Cloud Data Sense. Ningún otro servicio BlueXP es compatible con este tipo de despliegue, excepto con la cartera digital.

### Información general sobre el cloud

En una región de cloud sin Internet, puede usar BlueXP para poner en marcha sistemas Cloud Volumes ONTAP y detectar clústeres de ONTAP en las instalaciones (si hay una conexión de su entorno cloud a su entorno local). También puede utilizar Cloud Backup para realizar backups de volúmenes de Cloud Volumes ONTAP en regiones comerciales de AWS y Azure (actualmente, el backup no se admite en las regiones secretas de AWS y Azure). Ningún otro servicio BlueXP es compatible con este tipo de despliegue, excepto con la cartera digital.

La región del cloud puede ser una región en la que haya agencias estadounidenses seguras como AWS

C2S/SC2S, Azure IL6 o cualquier región comercial.

Estas instrucciones de instalación son específicas para el caso de uso descrito anteriormente. ["Obtenga información sobre otras formas de desplegar un conector"](#).

#### **Verifique los requisitos del host**

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

#### **Se requiere un host dedicado**

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

#### **CPU**

4 núcleos o 4 vCPU

#### **RAM**

14 GB

#### **Sistemas operativos compatibles**

- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6 y 8.7

El sistema Red Hat Enterprise Linux debe estar registrado con Red Hat Subscription Management. Si no está registrado, el sistema no puede acceder a los repositorios para actualizar el software necesario de terceros durante la instalación del conector.

El conector es compatible con las versiones en inglés de estos sistemas operativos.

#### **Hipervisor**

Un hipervisor de configuración básica o alojado certificado Ejecute CentOS o Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"^]

#### **Tipo de disco**

Se requiere un SSD

#### **Espacio en disco en /opt**

Debe haber 100 GiB de espacio disponibles

#### **Espacio en disco en /var**

Debe haber 20 GiB de espacio disponibles

#### **Motor Docker**

Se requiere Docker Engine versión 19 o posterior en el host antes de instalar el conector. ["Ver las instrucciones de instalación"](#)

#### **Instale el conector**

Después de verificar que tiene un host Linux compatible, puede obtener el software Connector y luego instalarlo.

## Privilegios requeridos

Se requieren privilegios de usuario raíz para instalar el conector.

## Pasos

1. Compruebe que docker está activado y en ejecución.

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. Descargue el instalador del conector para redes restringidas sin acceso a Internet desde el ["Sitio de soporte de NetApp"](#)
3. Copie el instalador en el host Linux.
4. Asigne permisos para ejecutar el script.

```
chmod +x /path/Cloud-Manager-Connector-offline-<version>
```

Donde <version> es la versión del conector que ha descargado.

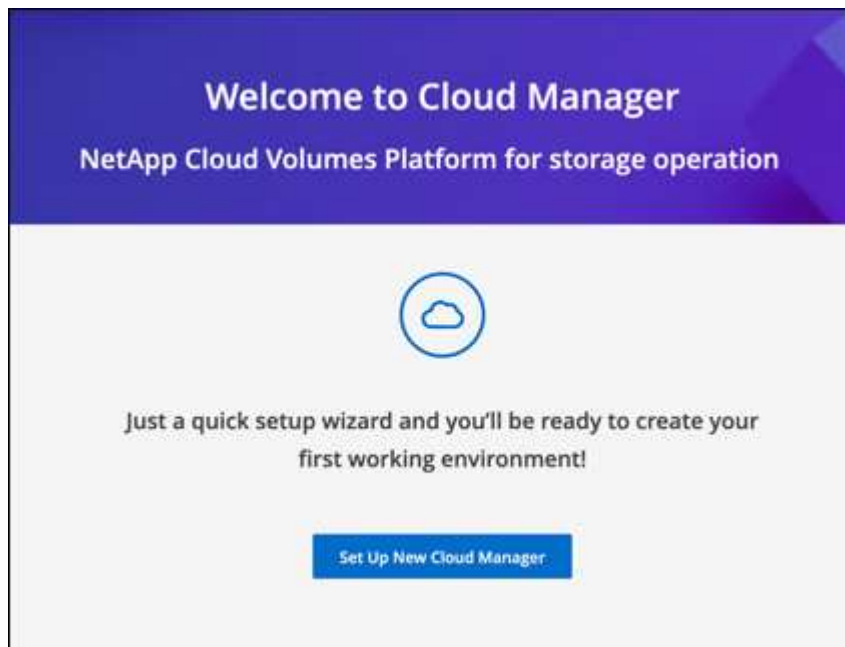
5. Ejecute el script de instalación:

```
sudo /path/Cloud-Manager-Connector-offline-<version>
```

Donde <version> es la versión del conector que ha descargado.

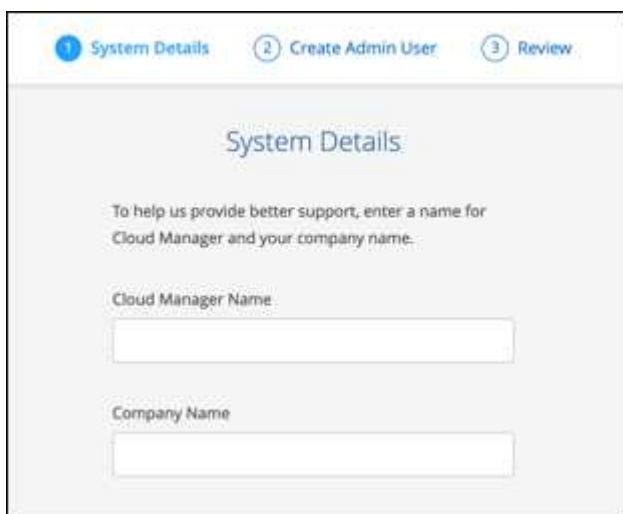
6. Abra un explorador web e introduzca `https://ipaddress[]` Donde *ipaddress* es la dirección IP del host Linux.

Debe ver la siguiente pantalla.



7. Haga clic en **Configurar nuevo BlueXP** y siga las indicaciones para configurar el sistema.

- **Detalles del sistema:** Introduzca un nombre para el conector y el nombre de su empresa.



- **Crear usuario administrador:** Cree el usuario administrador para el sistema.

Esta cuenta de usuario se ejecuta localmente en el sistema. No hay conexión con el servicio auth0 disponible a través de BlueXP.

- **Revisión:** Revise los detalles, acepte el acuerdo de licencia y haga clic en **Configurar**.

8. Inicie sesión en BlueXP con el usuario administrador que acaba de crear.

## Resultado

El conector ya está instalado y puede empezar a utilizar las funciones de BlueXP que están disponibles en una implementación de sitio oscuro.

## El futuro

En un entorno local:

- ["Detección de clústeres de ONTAP en las instalaciones"](#)
- ["Replique datos entre clústeres ONTAP en las instalaciones"](#)
- ["Realice backups de datos de volúmenes de ONTAP en las instalaciones en StorageGRID mediante Cloud Backup"](#)
- ["Analice datos de volúmenes de ONTAP en las instalaciones mediante Cloud Data Sense"](#)

En un entorno de cloud, puede hacerlo ["Ponga en marcha Cloud Volumes ONTAP"](#)

Cuando haya nuevas versiones del software del conector disponibles, estas se publicarán en el sitio de soporte de NetApp. ["Aprenda a actualizar el conector"](#).

## Búsqueda del ID del sistema de un conector

Para ayudarle a comenzar, es posible que su representante de NetApp le solicite el ID de sistema para un conector. El ID se utiliza normalmente para licencias y solución de problemas.

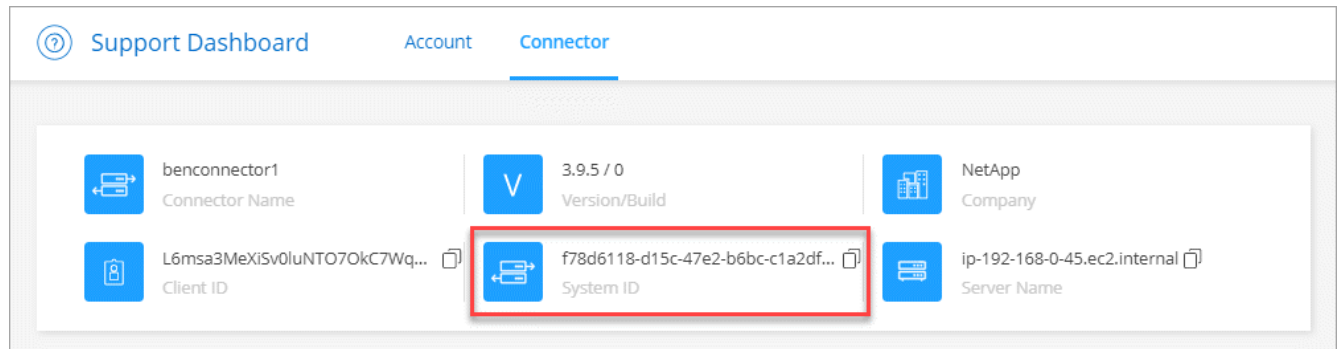
## Pasos



1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda.
2. Haga clic en **Soporte > conector**.

El ID del sistema aparece en la parte superior.

### ejemplo



## Gestión de conectores existentes

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

### Cambiar entre conectores

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

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

### Paso

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



BlueXP actualiza y muestra los entornos de trabajo asociados al conector seleccionado.

### Acceda a la interfaz de usuario local

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. Si accede a BlueXP desde una región gubernamental o un sitio que no tiene acceso saliente a Internet, deberá utilizar la interfaz de usuario local que se ejecuta en el conector.

#### Pasos

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

`https://ipaddress[]`

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

2. Introduzca su nombre de usuario y contraseña para iniciar sesión.

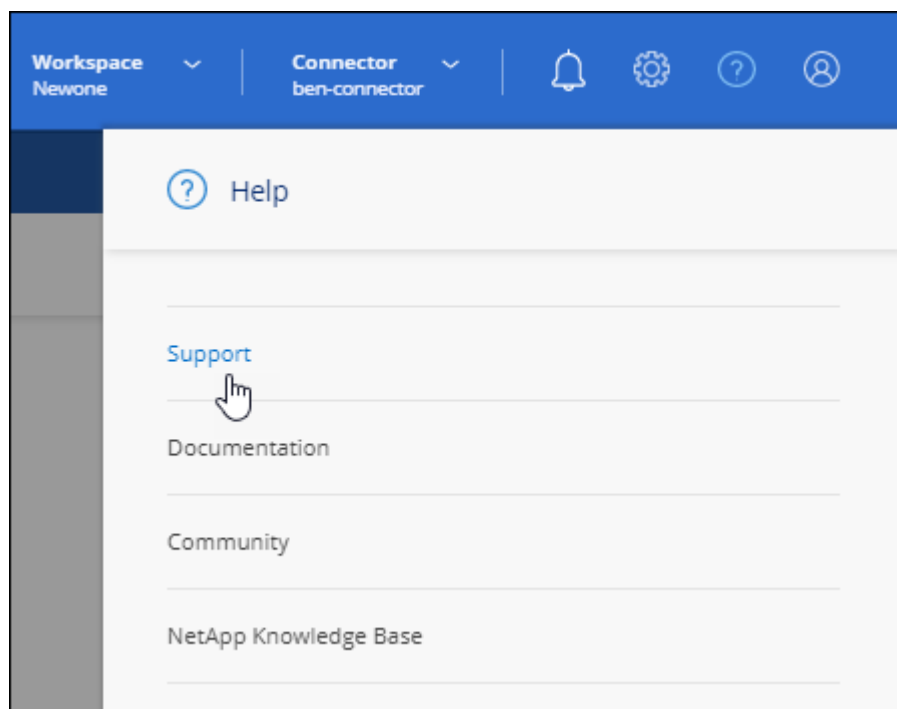
### Descargar o enviar un mensaje de AutoSupport

Si tiene problemas, es posible que el personal de NetApp le solicite enviar un mensaje de AutoSupport al soporte de NetApp para la solución de problemas.

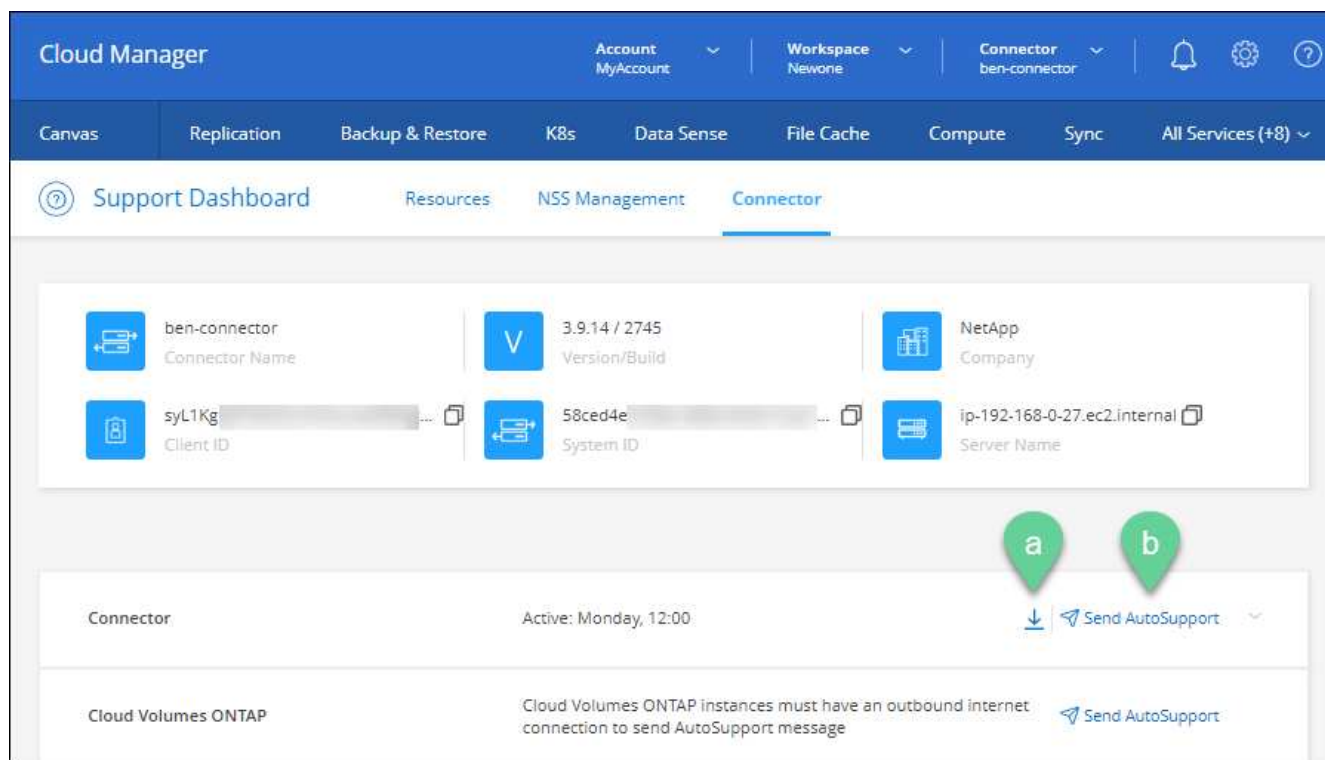
#### Pasos

1. Conéctese a la interfaz de usuario local de Connector, como se describe en la sección anterior.

2. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.



3. Haga clic en **conector**.
4. En función de cómo necesite enviar la información al soporte de NetApp, seleccione una de las siguientes opciones:
- a. Seleccione la opción para descargar el mensaje de AutoSupport en el equipo local. Luego, puede enviarlo al soporte de NetApp mediante un método preferido.
  - b. Haga clic en **Enviar AutoSupport** para enviar directamente el mensaje al soporte de NetApp.



## Conéctese a la máquina virtual de Linux

Si necesita conectarse a la VM de Linux en la que se ejecuta el conector, puede hacerlo utilizando las opciones de conectividad disponibles de su proveedor de cloud.

### AWS

Al crear la instancia de Connector en AWS, proporcionó una clave de acceso y una clave secreta de AWS. Es posible usar este par de claves para SSH a la instancia.

["AWS Docs: Conéctese a su instancia de Linux"](#)

### Azure

Cuando creó el conector VM en Azure, eligió autenticarse con una contraseña o una clave pública SSH. Utilice el método de autenticación que ha elegido para conectarse a la máquina virtual.

["Azure Docs: SSH en su máquina virtual"](#)

### Google Cloud

No puede especificar un método de autenticación al crear un conector en Google Cloud. Sin embargo, puede conectarse a la instancia de VM de Linux mediante Google Cloud Console o Google Cloud CLI (gcloud).

["Google Cloud Docs: Conexión a equipos virtuales Linux"](#)

## Aplicar actualizaciones de seguridad

Actualice el sistema operativo en el conector para asegurarse de que se ha aplicado la revisión con las actualizaciones de seguridad más recientes.

### Pasos

1. Acceda al shell de la CLI en el host del conector.
2. Ejecute los siguientes comandos con privilegios elevados:

```
sudo -s
service netapp-service-manager stop
yum -y update --security
service netapp-service-manager start
```

## Cambiar la dirección IP de un conector

Si es necesario para su empresa, puede cambiar la dirección IP interna y la dirección IP pública de la instancia de conector que asigna automáticamente su proveedor de cloud.

### Pasos

1. Siga las instrucciones del proveedor de cloud para cambiar la dirección IP local o la dirección IP pública (o ambas) de la instancia de Connector.
2. Si ha cambiado la dirección IP pública y necesita conectarse a la interfaz de usuario local que se ejecuta en el conector, reinicie la instancia del conector para registrar la nueva dirección IP con BlueXP.

3. Si cambió la dirección IP privada, actualice la ubicación de copia de seguridad de los archivos de configuración de Cloud Volumes ONTAP para que las copias de seguridad se envíen a la nueva dirección IP privada del conector.
  - a. Ejecute el siguiente comando desde la interfaz de línea de comandos de Cloud Volumes ONTAP para quitar el destino de backup actual:

```
system configuration backup settings modify -destination ""
```

- b. Vaya a BlueXP y abra el entorno de trabajo.
- c. Haga clic en el menú y seleccione **Avanzado > copias de seguridad de configuración**.
- d. Haga clic en **establecer destino de copia de seguridad**.

### Editar los URI de un conector

Agregar y quitar los URI de un conector.

#### Pasos

1. Haga clic en el menú desplegable **conector** del encabezado BlueXP.
2. Haga clic en **Administrar conectores**.
3. Haga clic en el menú de acción de un conector y haga clic en **Editar URI**.
4. Agregue y elimine URIs y, a continuación, haga clic en **aplicar**.

### Solucione los fallos de descarga al utilizar una puerta de enlace NAT de Google Cloud

El conector descarga automáticamente las actualizaciones de software de Cloud Volumes ONTAP. La descarga puede fallar si la configuración utiliza una puerta de enlace de NAT de Google Cloud. Puede corregir este problema limitando el número de partes en las que se divide la imagen de software. Este paso se debe completar mediante la API de BlueXP.

#### Paso

1. Envíe una solicitud PUT a /occm/config con el siguiente JSON como cuerpo:

```
{
  "maxDownloadSessions": 32
}
```

El valor para *maxDownloadSessions* puede ser 1 o cualquier entero mayor que 1. Si el valor es 1, la imagen descargada no se dividirá.

Tenga en cuenta que 32 es un valor de ejemplo. El valor que debe utilizar depende de la configuración de NAT y del número de sesiones que puede tener simultáneamente.

["Obtenga más información acerca de la llamada a la API /occm/config"](#).

### Actualice el conector en una ubicación sin acceso a Internet

Si usted ["Se instaló el conector en una ubicación en la que no hay acceso a Internet"](#), Puede actualizar el

conector cuando haya una versión más reciente disponible en el sitio de soporte de NetApp.

El conector debe reiniciarse durante el proceso de actualización para que la interfaz de usuario no esté disponible durante la actualización.

#### Pasos

1. Descargue el software del conector de ["Sitio de soporte de NetApp"](#).
2. Copie el instalador en el host Linux.
3. Asigne permisos para ejecutar el script.

```
chmod +x /path/cloud-manager-connector-offline-<version>
```

Donde <version> es la versión del conector que ha descargado.

4. Ejecute el script de instalación:

```
sudo /path/cloud-manager-connector-offline-<version>
```

Donde <version> es la versión del conector que ha descargado.

5. Una vez finalizada la actualización, puede verificar la versión del conector en **Ayuda > Soporte > conector**.

### ¿Qué pasa con las actualizaciones de software en los hosts que tienen acceso a Internet?

El conector actualiza automáticamente su software a la última versión, siempre que tenga acceso saliente a Internet para obtener la actualización de software.

#### Quitar conectores de BlueXP

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

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

- Esta acción no elimina la máquina virtual.
- Esta acción no se puede revertir—una vez que se quita un conector de BlueXP, no se puede volver a agregar

#### Pasos

1. Haga clic en el menú desplegable **conector** del encabezado BlueXP.
2. Haga clic en **Administrar conectores**.
3. Haga clic en el menú de acción de un conector inactivo y haga clic en **Quitar conector**.



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

### Resultado

BlueXP quita el conector de sus registros.

### Desinstale el software del conector

Desinstale el software del conector para solucionar problemas o para quitar el software del host de forma permanente. Los pasos que debe seguir dependen de si ha instalado el conector en un host que tenga acceso a Internet o un host en una red restringida que no tenga acceso a Internet.

#### Desinstale desde un host con acceso a Internet

El conector en línea incluye una secuencia de comandos de desinstalación que puede utilizar para desinstalar el software.

#### Paso

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

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

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

#### Desinstale desde un host sin acceso a Internet

Use estos comandos si descargó el software del conector del sitio de soporte de NetApp y lo instaló en una red restringida que no tiene acceso a Internet.

#### Paso

1. Desde el host Linux, ejecute los siguientes comandos:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

## Gestión de un certificado HTTPS para un acceso seguro

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

### Antes de empezar

Debe crear un conector para poder cambiar la configuración de BlueXP. ["Vea cómo"](#).

### Instalar un certificado HTTPS

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

#### Pasos

1. En la parte superior derecha de la consola BlueXP, 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	<p>a. Introduzca el nombre de host o DNS del host del conector (su nombre común) y, a continuación, haga clic en <b>generar CSR</b>.</p> <p>BlueXP muestra una solicitud de firma de certificado.</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. Cargue el archivo de certificado y, a continuación, haga clic en <b>instalar</b>.</p>
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

Ahora BlueXP utiliza el certificado firmado por CA para proporcionar acceso HTTPS seguro. La siguiente imagen muestra una cuenta de BlueXP configurada para un acceso seguro:





## Renovación del certificado HTTPS de BlueXP

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

### Pasos

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

Se muestra información sobre el certificado BlueXP, incluida la fecha de caducidad.

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

### Resultado

BlueXP utiliza el nuevo certificado firmado por CA para proporcionar acceso HTTPS seguro.

## Configure un conector para que utilice un servidor proxy

Si las directivas de la empresa requieren que utilice un servidor proxy para todas las comunicaciones a Internet, deberá configurar los conectores para que utilicen ese servidor proxy. Si no configuró un conector para que utilice un servidor proxy durante la instalación, puede configurar el conector para que utilice ese servidor proxy en cualquier momento.

BlueXP admite HTTP y HTTPS. El servidor proxy puede estar en la nube o en la red.

Configurar el conector para que utilice un servidor proxy proporciona acceso saliente a Internet si no hay disponible una dirección IP pública o una puerta de enlace NAT. Este servidor proxy sólo proporciona el

conector con una conexión saliente. No ofrece conectividad para los sistemas Cloud Volumes ONTAP.

Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes AutoSupport, BlueXP configura automáticamente esos sistemas Cloud Volumes ONTAP para que utilicen un servidor proxy incluido con el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

### Activar un proxy en un conector

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

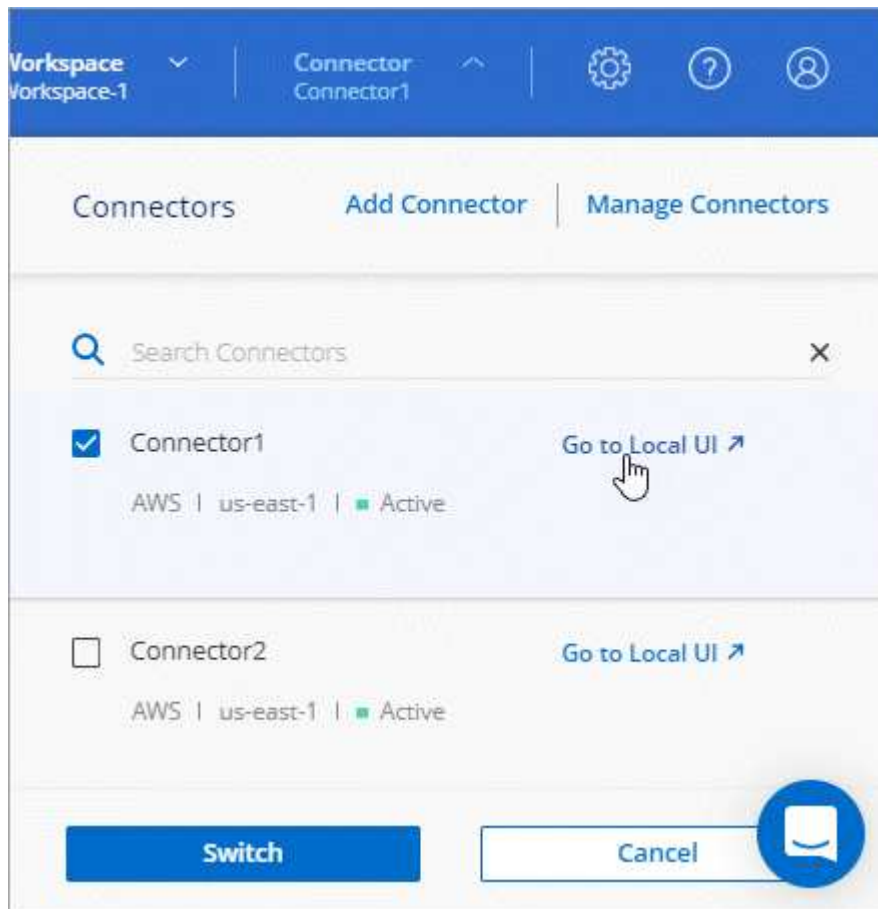
Tenga en cuenta que esta operación reinicia el conector. Asegúrese de que el conector no realiza ninguna operación antes de continuar.

### Pasos

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

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

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



La interfaz BlueXP que se ejecuta en el conector se carga en una nueva pestaña del navegador.

3. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **Configuración del conector**.



4. En **General**, haga clic en **Configuración de proxy HTTP**.
5. Configure el proxy:
  - a. Haga clic en **Activar proxy**.
  - b. Especifique el servidor con la sintaxis `http://address:port[]` o `https://address:port[]`
  - c. Especifique un nombre de usuario y una contraseña si se requiere autenticación básica para el servidor
  - d. Haga clic en **Guardar**.



BlueXP no admite contraseñas que incluyan el carácter @.

### Habilite el tráfico de API directo

Si ha configurado un conector para utilizar un servidor proxy, puede habilitar el tráfico API directo en el conector para enviar llamadas API directamente a servicios de proveedores de cloud sin pasar por el proxy. Esta opción es compatible con conectores que se ejecutan en AWS, en Azure o en Google Cloud.

Si deshabilitó el uso de vínculos privados de Azure con Cloud Volumes ONTAP y utiliza extremos de servicio, debe habilitar el tráfico de API directo. De lo contrario, el tráfico no se enrutará correctamente.

["Obtenga más información sobre el uso de un enlace privado de Azure o extremos de servicio con Cloud Volumes ONTAP"](#)

### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **Configuración del conector**.



2. En **General**, haga clic en **Support Direct API Traffic**.
3. Haga clic en la casilla de verificación para activar la opción y, a continuación, haga clic en **Guardar**.

### Configuración predeterminada del conector

Es posible que desee obtener más información sobre el conector antes de implementarlo o si necesita solucionar cualquier problema.

## Configuración predeterminada con acceso a Internet

Los siguientes detalles de configuración se aplican si ha implementado el conector desde BlueXP, desde el mercado del proveedor de la nube o si ha instalado manualmente el conector en un host Linux local que tenga acceso a Internet.

### Detalles de AWS

Si implementó el conector desde BlueXP o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de instancia de EC2 es t3.xlarge.
- El sistema operativo de la imagen es Red Hat Enterprise Linux 7.6 (HVM).

El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- El nombre de usuario de la instancia de EC2 Linux es ec2-user.
- El disco del sistema predeterminado es un disco gp2 de 100 GiB.

### Detalles de Azure

Si implementó el conector desde BlueXP o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de máquina virtual es DS3 v2.
- El sistema operativo de la imagen es CentOS 7.6.

El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- El disco del sistema predeterminado es un disco SSD premium de 100 GiB.

### Detalles de Google Cloud

Si implementó el conector desde BlueXP o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- La instancia del equipo virtual es n2-standard-4.
- El sistema operativo de la imagen es Red Hat Enterprise Linux 8.6.

El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- El disco del sistema predeterminado es un disco SSD persistente de 100 GiB.

### Carpeta de instalación

La carpeta de instalación del conector se encuentra en la siguiente ubicación:

`/opt/aplicación/netapp/cloudmanager`

### Archivos de registro

Los archivos de registro se encuentran en las siguientes carpetas:

- `/opt/application/netapp/cloudmanager/log o.`

- /opt/application/netapp/service-manager-2/logs (a partir de las nuevas instalaciones de 3.9.23)

Los registros de estas carpetas proporcionan detalles sobre las imágenes de conector y Docker.

- /opt/aplicación/netapp/cloudmanager/docker\_occm/data/log

Los registros de esta carpeta proporcionan detalles sobre los servicios en la nube y el servicio BlueXP que se ejecuta en el conector.

### Servicio de conectores

- El servicio BlueXP se llama occm.
- El servicio occm depende del servicio MySQL.

Si el servicio MySQL está inactivo, entonces el servicio occm también está inactivo.

### Puertos

El conector utiliza los siguientes puertos en el host Linux:

- 80 para acceso HTTP
- 443 para acceso HTTPS

### Configuración predeterminada sin acceso a Internet

La siguiente configuración se aplica si instaló manualmente el conector en un host Linux local que no tiene acceso a Internet. ["Obtenga más información sobre esta opción de instalación"](#).

- La carpeta de instalación del conector se encuentra en la siguiente ubicación:

/opt/aplicación/netapp/ds

- Los archivos de registro se encuentran en las siguientes carpetas:

/var/lib/docker/volumes/ds\_occmdata/\_data/log

Los registros de esta carpeta proporcionan detalles sobre las imágenes de conector y Docker.

- Todos los servicios se ejecutan en contenedores Docker

Los servicios dependen del servicio docker Runtime que se esté ejecutando

- El conector utiliza los siguientes puertos en el host Linux:
  - 80 para acceso HTTP
  - 443 para acceso HTTPS

## Gestionar suscripciones y contratos de PAYGO

Al suscribirse a BlueXP desde el mercado de un proveedor de la nube, se le redirigirá al sitio web de BlueXP donde necesita guardar su suscripción y asociarla a cuentas específicas. Una vez que se haya suscrito, cada suscripción estará disponible para

administrar desde Digital Wallet.

### Ver sus suscripciones

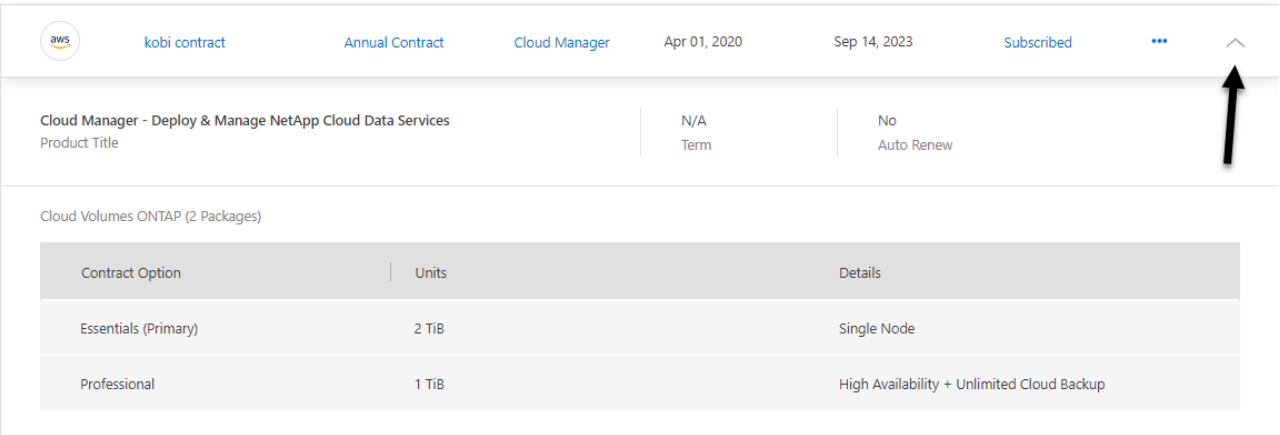
La cartera digital proporciona detalles sobre cada suscripción a PAYGO y el contrato anual asociado con su cuenta BlueXP y con Astra (Astra utiliza el servicio de carga de BlueXP).


#### Pasos


1. En el menú de navegación de BlueXP, seleccione **Gobierno > cartera digital**.
2. Seleccione **Suscripciones**.

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

3. Cuando vea la información sobre sus suscripciones, puede interactuar con los detalles de la tabla de la siguiente manera:
  - Expanda una fila para ver más detalles.



	kobi contract	Annual Contract	Cloud Manager	Apr 01, 2020	Sep 14, 2023	Subscribed	...	^
Cloud Manager - Deploy & Manage NetApp Cloud Data Services Product Title				N/A Term	No Auto Renew			
Cloud Volumes ONTAP (2 Packages)								
Contract Option			Units	Details				
Essentials (Primary)			2 TiB	Single Node				
Professional			1 TiB	High Availability + Unlimited Cloud Backup				

- Haga clic en  para elegir las columnas que aparecen en la tabla.

Tenga en cuenta que las columnas término y renovación automática no aparecen de forma predeterminada. La columna renovación automática muestra información de renovación únicamente para los contratos de Azure.

Tenga en cuenta lo siguiente acerca de lo que puede ver en la tabla:

#### Fecha de inicio

La fecha de inicio es cuando ha asociado correctamente la suscripción a su cuenta y se ha iniciado la carga.

#### N.A.

Si observa N/A en la tabla, la información no está disponible en la API del proveedor de cloud en este momento.

#### Contratos

- Si expande los detalles de un contrato, el monedero digital muestra lo que está disponible para su plan actual: Las opciones de contrato y las unidades (capacidad o número de nodos).
- El monedero digital identificará la fecha de finalización y si el contrato se renovará pronto, finalizará pronto o si ya ha finalizado.

- Si tiene un contrato de AWS y ha cambiado alguna de las opciones del contrato tras la fecha de inicio, asegúrese de validar las opciones de contrato desde AWS.




## Gestione sus suscripciones

Puede gestionar sus suscripciones desde Digital Wallet cambiando el nombre de una suscripción y eligiendo las cuentas asociadas a la suscripción.

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

### Pasos

1. En el menú de navegación de BlueXP, seleccione **Gobierno > cartera digital**.
2. Seleccione **Suscripciones**.
3. Haga clic en el menú de acciones de la fila correspondiente a la suscripción que desea administrar.

Provider	Name	Type	Service	Start Date	End Date	Status	
	aws-sub-a2	PAYGO	Cloud Manager	Apr 02, 2020	N/A	Subscribed	⋮
	Aleksey_aws_marketplace	Annual Contract	Astra	Oct 18, 2022	Oct 18, 2023		⋮
	By Capacity By Node 3	PAYGO	Cloud Manager	Mar 31, 2020	N/A	Subscribed	⋮

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

## Almacenamiento en cloud detectado

### Gestión de bloques de Amazon S3

Después de instalar un conector en AWS, BlueXP puede descubrir automáticamente información sobre los cubos de Amazon S3 que residen en la cuenta de AWS donde está instalado el conector. Se añade un entorno de trabajo de Amazon S3 al lienzo para poder ver esta información.



Puede ver detalles sobre sus bloques de S3, incluida la región, la política de acceso, la cuenta, la capacidad total y utilizada, etc. Estos bloques se pueden usar como destinos para las operaciones Cloud Backup, Cloud Tiering o Cloud Sync. Además, puede usar Cloud Data Sense para analizar estos bloques.

Una función recién añadida ahora permite crear y editar bloques S3. ["Vaya aquí para ver cómo puede ver, crear y gestionar sus buckets de S3 con BlueXP."](#)

## Ver sus cuentas de Azure Blob

Después de instalar un conector en Azure, BlueXP puede descubrir automáticamente información sobre las cuentas de almacenamiento de Azure que residen en las suscripciones de Azure donde está instalado el conector. Se añade un entorno de trabajo de Azure Blob al lienzo para que pueda ver esta información.

Puede ver detalles acerca de sus cuentas de almacenamiento de Azure, incluidas la ubicación, el grupo de recursos, la capacidad total y utilizada, entre otros. Estas cuentas se pueden usar como destinos para las operaciones Cloud Backup, Cloud Tiering o Cloud Sync.

### Pasos

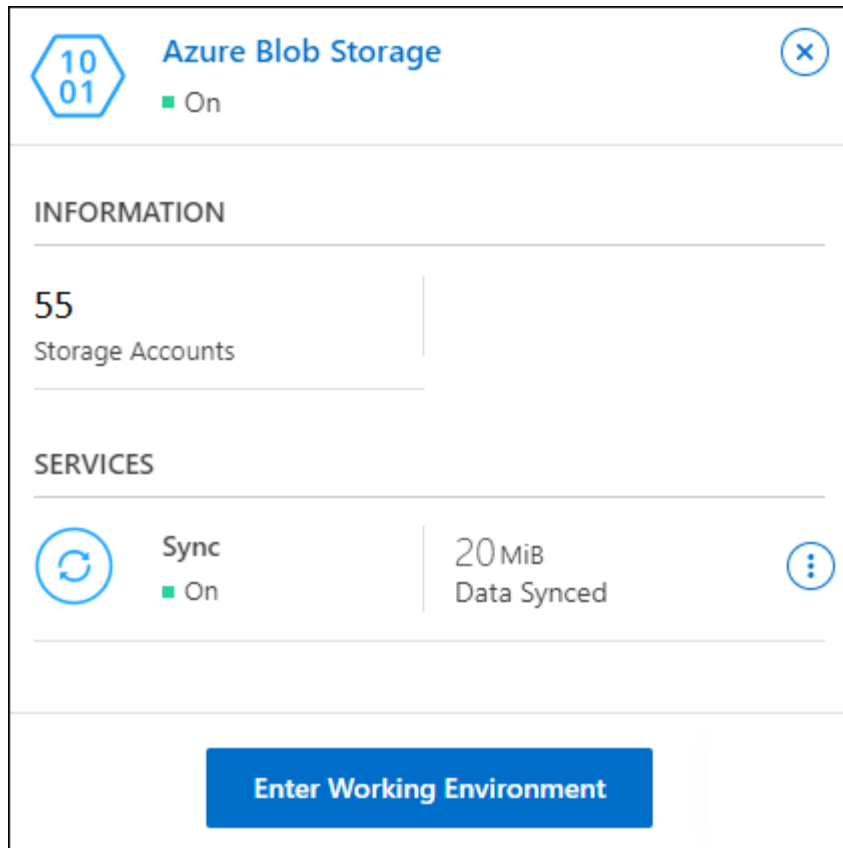
1. ["Instale un conector"](#) En la cuenta de Azure donde desea ver las cuentas de almacenamiento de Azure.
2. En el menú de navegación, selecciona **almacenamiento > Canvas**.

Debería ver automáticamente un entorno de trabajo de Azure Blob un poco después.



3. Haga clic en el entorno de trabajo y seleccione una acción en el panel derecho.





4. Haga clic en **Sincronizar datos** para sincronizar los datos con o desde el almacenamiento de Azure Blob.

Para obtener información detallada, consulte ["La descripción del servicio Cloud Sync"](#).

5. Haga clic en **Entrar en entorno de trabajo** para ver detalles sobre las cuentas de almacenamiento de Azure en sus Blobs de Azure.

Azure blob

Overview

637

Total Storage Accounts

1.5

TiB

Total Capacity

16

Total Locations

637

Storage Accounts

Storage Account Name	Subscription	Location	Creation Date	Resource Group	Blob Capacity
ovu8llxvqdfypxn	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	170 B
rootsa9ktpjzcm	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	950.22 GiB
scvdwjcwehswli	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	22.12 MiB
65qtx0smegmq2vt	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	170 B
bu9klxthymr1be	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	1.01 MiB
8jzsvybvjiwieww8	OCCM QA1	Canada Central	December 12, 2019	aff1-rg	170 B

## Visualización de sus buckets de Google Cloud Storage

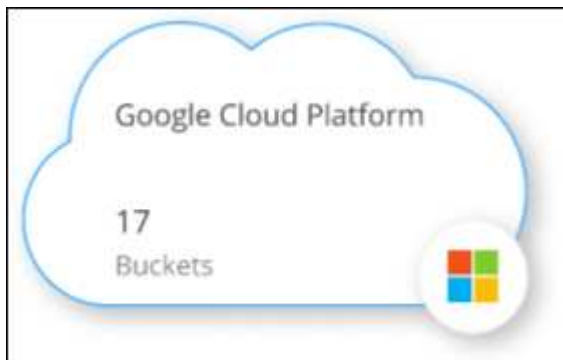
Después de instalar un conector en Google Cloud, BlueXP puede descubrir automáticamente información sobre los cubos de Google Cloud Storage que residen en la cuenta de Google donde está instalado el conector. Se añade un entorno de trabajo de Google Cloud Storage al lienzo para que puedas ver esta información.

Puede ver detalles sobre sus buckets de Google Cloud Storage, donde se incluyen la ubicación, el estado de acceso, la clase de almacenamiento, la capacidad total y utilizada, entre otros. Estos bloques se pueden usar como destinos para las operaciones Cloud Backup, Cloud Tiering o Cloud Sync.

### Pasos

1. "[Instale un conector](#)" En la cuenta de Google, donde desea ver sus bloques de Google Cloud Storage.
2. En el menú de navegación, selecciona **almacenamiento > Canvas**.

Verá automáticamente un entorno de trabajo de Google Cloud Storage poco después.



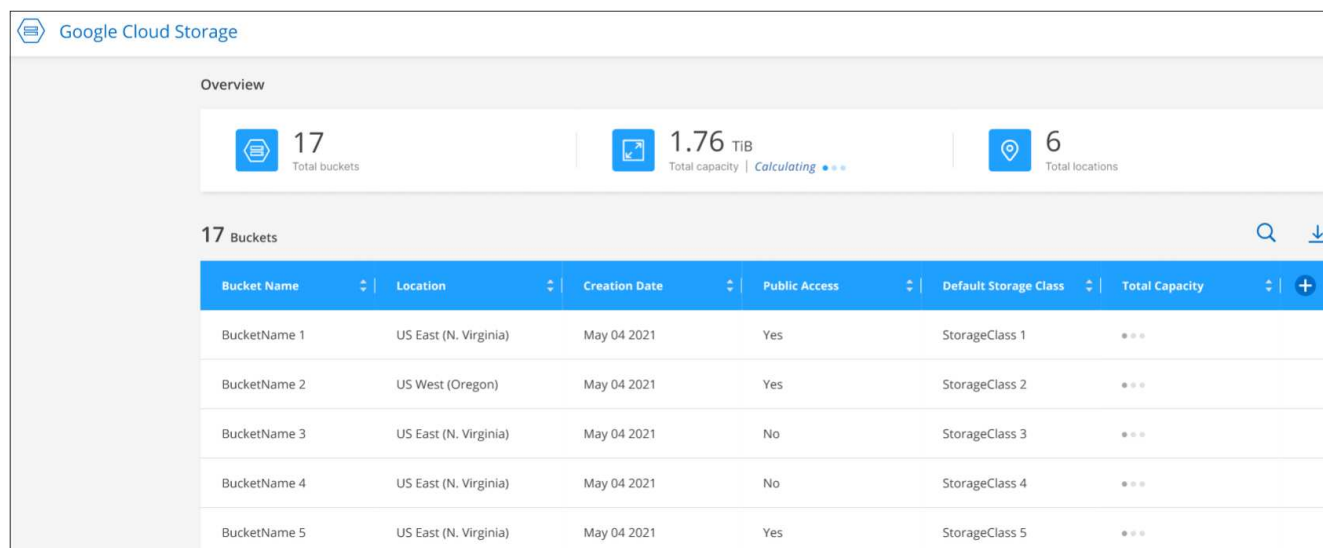
3. Haga clic en el entorno de trabajo y seleccione una acción en el panel derecho.



4. Haga clic en **Sincronizar datos** para sincronizar los datos con o desde los cubos de Google Cloud Storage.

Para obtener información detallada, consulte ["La descripción del servicio Cloud Sync"](#).

5. Haga clic en **Entrar en entorno de trabajo** para ver los detalles de los cubos de su cuenta de Google.



Bucket Name	Location	Creation Date	Public Access	Default Storage Class	Total Capacity
BucketName 1	US East (N. Virginia)	May 04 2021	Yes	StorageClass 1	***
BucketName 2	US West (Oregon)	May 04 2021	Yes	StorageClass 2	***
BucketName 3	US East (N. Virginia)	May 04 2021	No	StorageClass 3	***
BucketName 4	US East (N. Virginia)	May 04 2021	No	StorageClass 4	***
BucketName 5	US East (N. Virginia)	May 04 2021	Yes	StorageClass 5	***

## Credenciales de AWS

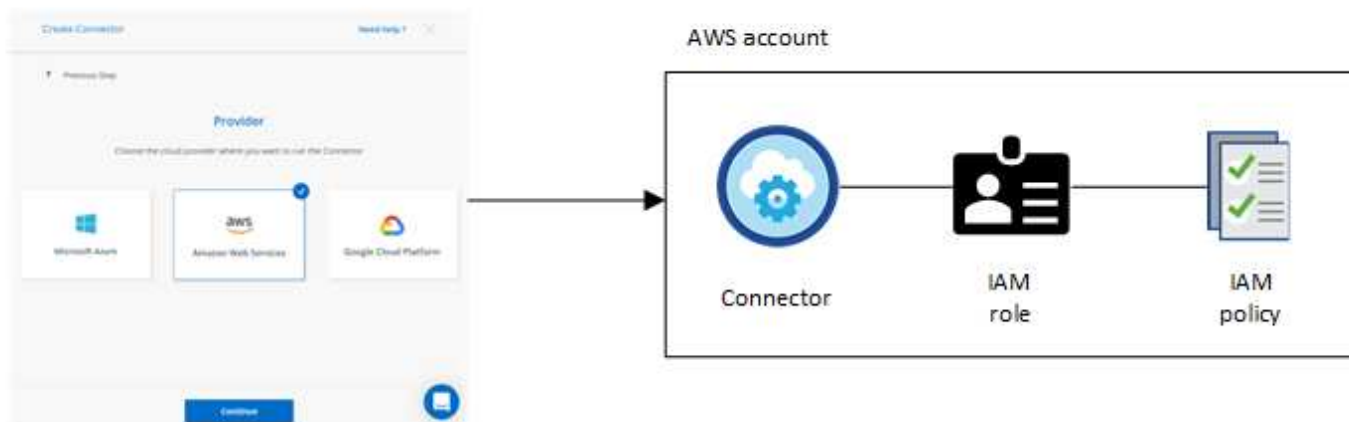
### Credenciales y permisos de AWS

BlueXP le permite elegir las credenciales de AWS que deben utilizarse 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 implantar un conector de BlueXP, debe proporcionar el ARN de una función de IAM o claves de acceso para un usuario de IAM. El método de autenticación que utilice debe tener los permisos necesarios para implementar la instancia de Connector en AWS. Los permisos necesarios se enumeran en la ["La política de implementación de conectores para AWS"](#).

Cuando BlueXP inicia la instancia de Connector en AWS, crea una función IAM y un perfil de instancia para la instancia. También adjunta una directiva que proporciona al conector permisos para administrar recursos y procesos dentro de esa cuenta de AWS. ["Revise cómo BlueXP utiliza los permisos"](#).



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

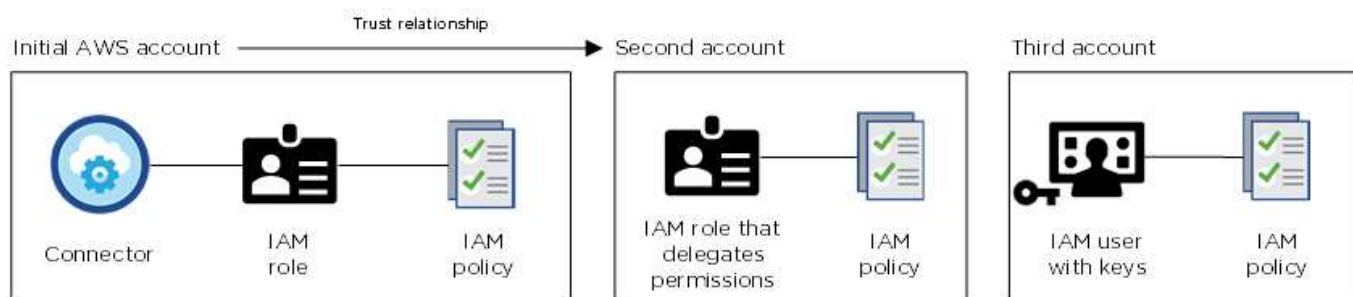
Details & Credentials			
Instance Profile		QA Subscription	<a href="#">Edit Credentials</a>
Credentials	Account ID	Marketplace Subscription	

## Credenciales adicionales de AWS

Existen dos formas de añadir credenciales adicionales de AWS.

### Agregar credenciales de AWS a un conector existente

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 ["Agregue las credenciales de cuenta a BlueXP"](#) 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:

**Edit Credentials & Add Subscription**

---

Associate Subscription to Credentials ⓘ

Credentials

keys   Account ID:
Instance Profile   Account ID:

casaba QA subscription

+ Add Subscription

Apply Cancel

#### **Añada credenciales de AWS directamente a BlueXP**

Agregar nuevas credenciales de AWS a BlueXP proporciona los permisos necesarios para crear y gestionar un entorno de trabajo FSX para ONTAP o crear un conector.

#### **¿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 BlueXP. 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.

Para las implementaciones locales, no puede configurar una función de IAM para el sistema BlueXP, pero puede proporcionar permisos como lo haría para cuentas de AWS adicionales.

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

Como se ha descrito anteriormente, BlueXP permite proporcionar credenciales de AWS de varias maneras: Una función IAM asociada a la instancia de Connector, asumiendo una función IAM en una cuenta de confianza o proporcionando claves de acceso de AWS.

Con las dos primeras opciones, BlueXP utiliza el Servicio de token de seguridad de AWS para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica, es automático y seguro.

Si proporciona a BlueXP claves de acceso de AWS, debe rotar las claves actualizándolas en BlueXP a intervalos regulares. Este es un proceso completamente manual.

## Gestione las credenciales y suscripciones de AWS para BlueXP

Añada y gestione credenciales de AWS para que BlueXP tenga los permisos que necesita para implementar y gestionar recursos cloud en sus cuentas de AWS. Si administra varias suscripciones de AWS, puede asignar cada una de ellas a diferentes credenciales de AWS desde la página Credentials.

### Descripción general

Puede añadir credenciales de AWS a un conector existente o directamente a BlueXP:

- Agregue credenciales de AWS adicionales a un conector existente

Añadir credenciales de AWS a un conector existente proporciona los permisos necesarios para gestionar recursos y procesos dentro de su entorno de cloud público. [Aprenda a añadir credenciales de AWS a un conector](#).

- Añada las credenciales de AWS a BlueXP para crear un conector

La adición de nuevas credenciales de AWS a BlueXP proporciona a BlueXP los permisos necesarios para crear un conector. [Aprenda a añadir credenciales de AWS a BlueXP](#).

- Añada credenciales de AWS a BlueXP para FSX para ONTAP

La adición de nuevas credenciales de AWS a BlueXP proporciona a BlueXP los permisos necesarios para crear y gestionar FSX para ONTAP. ["Aprenda a configurar permisos para FSX para ONTAP"](#)

### Cómo rotar credenciales

BlueXP le permite proporcionar credenciales de AWS de varias maneras: Una función IAM asociada a 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, BlueXP utiliza el Servicio de token de seguridad de AWS para obtener credenciales temporales que giran constantemente. Este proceso es la mejor práctica porque es automático y seguro.

Si proporciona a BlueXP claves de acceso de AWS, debe rotar las claves actualizándolas en BlueXP a intervalos regulares. Este es un proceso completamente manual.

### Agregar credenciales a un conector

Añada las credenciales de AWS a un conector para que tenga los permisos necesarios para gestionar los recursos y procesos en su entorno de cloud público. Puede proporcionar el ARN de un rol IAM en otra cuenta o proporcionar claves de acceso de AWS.

### Conceder permisos

Antes de agregar credenciales de AWS a un conector, debe proporcionar los permisos necesarios. Los permisos permiten a BlueXP administrar recursos y procesos dentro de esa cuenta de AWS. La forma en que proporcione los permisos depende de si desea proporcionar BlueXP con el ARN de una función en una cuenta de confianza o claves de AWS.



Si implementó un conector desde BlueXP, BlueXP agregó automáticamente credenciales de AWS para la cuenta en la que implementó el conector. Esta cuenta inicial no se agrega si implementó el conector desde AWS Marketplace o si instaló manualmente el software Connector en un sistema existente. ["Obtenga más información acerca de los permisos y credenciales de AWS"](#).

## opciones

- [Conceda permisos asumiendo una función IAM en otra cuenta](#)
- [Conceda permisos proporcionando claves AWS](#)

### Conceda permisos asumiendo una función IAM en otra cuenta

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 BlueXP el ARN de las funciones de IAM de las cuentas de confianza.

Si el conector está instalado en las instalaciones, no puede utilizar este método de autenticación. Debe usar claves AWS.

#### Pasos

1. Vaya a la consola IAM de la cuenta de destino en la que desea proporcionar permisos al conector.
2. En Access Management, haga clic en **roles > Crear función** y siga los pasos para crear la función.

No olvide hacer lo siguiente:

- En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
  - Seleccione **otra cuenta de AWS** e introduzca el ID de la cuenta en la que reside la instancia de Connector.
  - Cree las directivas necesarias copiando y pegando el contenido de ["Políticas de IAM para el conector"](#).
3. Copie el rol ARN del rol IAM para que pueda pegarlo en BlueXP más adelante.

#### Resultado

La cuenta ahora tiene los permisos necesarios. [Ahora puede agregar las credenciales a un conector](#).

### Conceda permisos proporcionando claves AWS

Si desea proporcionar BlueXP con claves AWS para un usuario de IAM, debe conceder los permisos necesarios a ese usuario. La política IAM de BlueXP define las acciones y los recursos de AWS que BlueXP puede utilizar.

Debe utilizar este método de autenticación si el conector está instalado en las instalaciones. No se puede utilizar la función IAM.

#### Pasos

1. Desde la consola IAM, cree directivas copiando y pegando el contenido de ["Políticas de IAM para el conector"](#).

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

2. Asocie las políticas 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 agregar las credenciales a un conector.](#)

## Añada las credenciales

Después de proporcionar una cuenta de AWS con los permisos necesarios, puede agregar las credenciales de esa cuenta a un conector existente. Esto permite iniciar sistemas Cloud Volumes ONTAP en esa cuenta con el mismo conector.

## Antes de empezar

Si acaba de crear estas credenciales en su proveedor de cloud, es posible que transcurran unos minutos hasta que estén disponibles para su uso. Espere unos minutos antes de agregar las credenciales a BlueXP.

## Pasos

1. Asegúrese de que el conector correcto está seleccionado actualmente en BlueXP.
2. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.



3. Haga clic en **Agregar credenciales** y siga los pasos del asistente.
  - a. **Ubicación de credenciales:** Seleccione **Servicios Web de Amazon > conector**.
  - b. **Definir credenciales:** Proporcione el ARN (nombre de recurso de Amazon) de una función de IAM de confianza, o introduzca una clave de acceso de AWS y una clave secreta.
  - c. **Suscripción al mercado:** Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

Para pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO) o con un contrato anual, las credenciales de AWS deben estar asociadas con una suscripción a Cloud Volumes ONTAP desde AWS Marketplace.

- d. **Revisión:** Confirme los detalles acerca de las nuevas credenciales y 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:



Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

keys   Account ID:
Instance Profile   Account ID:

casaba QA subscription

+ Add Subscription

Apply Cancel

### Agregar credenciales a BlueXP para crear un conector

Agregue las credenciales de AWS a BlueXP proporcionando el ARN de una función IAM que proporciona a BlueXP los permisos necesarios para crear un conector. Puede elegir estas credenciales al crear un conector nuevo.

#### Configure el rol IAM

Configure una función de IAM que permita al SaaS BlueXP asumir la función.

#### Pasos

1. Vaya a la consola IAM de la cuenta de destino.
2. En Access Management, haga clic en **roles > Crear función** y siga los pasos para crear la función.

No olvide hacer lo siguiente:

- En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
- Seleccione **otra cuenta de AWS** e introduzca el ID del SaaS BlueXP: 952013314444
- Cree una directiva que incluya los permisos necesarios para crear un conector.
  - ["Consulte los permisos necesarios para FSX para ONTAP"](#)
  - ["Ver la directiva de despliegue del conector"](#)

3. Copie el rol ARN de la función IAM para que pueda pegarlo en BlueXP en el siguiente paso.

#### Resultado

El rol IAM ahora tiene los permisos necesarios. [Ahora puede agregarla a BlueXP](#).

## Añada las credenciales

Después de proporcionar la función IAM con los permisos necesarios, agregue el rol ARN a BlueXP.

### Antes de empezar

Si acaba de crear la función IAM, puede tardar unos minutos en estar disponible. Espere unos minutos antes de agregar las credenciales a BlueXP.

### Pasos

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



2. Haga clic en **Agregar credenciales** y siga los pasos del asistente.
  - a. **Ubicación de credenciales:** Seleccione **Servicios Web de Amazon > BlueXP**.
  - b. **Definir credenciales:** Proporcionar el ARN (nombre de recurso de Amazon) de la función IAM.
  - c. **Revisión:** Confirme los detalles acerca de las nuevas credenciales y haga clic en **Agregar**.

### Resultado

Ahora puede utilizar las credenciales al crear un conector nuevo.

## Asocie una suscripción a AWS

Después de añadir sus credenciales de AWS a BlueXP, puede asociar una suscripción a AWS Marketplace con estas credenciales. La suscripción le permite pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO) o utilizar un contrato anual, y utilizar 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 BlueXP:

- No asoció una suscripción cuando agregó inicialmente las credenciales a BlueXP.
- Desea sustituir una suscripción existente de AWS Marketplace por una nueva suscripción.

### Lo que necesitará

Debe crear un conector para poder cambiar la configuración de BlueXP. ["Aprenda a crear un conector"](#).

### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Suscripción asociada**.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y haga clic en **asociado**.
4. Para asociar las credenciales con una nueva suscripción, haga clic en **Agregar suscripción > continuar** y siga los pasos del AWS Marketplace:
  - a. Haga clic en **Ver opciones de compra**.
  - b. Haga clic en **Suscribirse**.
  - c. Haga clic en **Configurar su cuenta**.

Se le redirigirá al sitio web de BlueXP.

- d. Desde la página **asignación de suscripción**:

- Seleccione las cuentas de NetApp a las que desea asociar esta suscripción.
- En el campo **sustituir suscripción existente**, elija si desea sustituir automáticamente la suscripción existente para una cuenta con esta nueva suscripción.

BlueXP reemplaza la suscripción existente para todas las credenciales de la cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Haga clic en **Guardar**.

En el siguiente vídeo se muestran los pasos para suscribirse desde Google Cloud Marketplace:

► [https://docs.netapp.com/es-es/cloud-manager-setup-admin//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/es-es/cloud-manager-setup-admin//media/video_subscribing_aws.mp4) (video)

## Editar credenciales

Edite sus credenciales de AWS en BlueXP cambiando el tipo de cuenta (las claves de AWS o asumen la función), editando el nombre o actualizando las credenciales (las claves o el rol ARN).



No se pueden editar las credenciales de un perfil de instancia asociado a una instancia de conector.

## Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Editar credenciales**.
3. Realice los cambios necesarios y, a continuación, haga clic en **aplicar**.

### Eliminación de credenciales

Si ya no necesita un conjunto de credenciales, puede eliminarlas de BlueXP. Sólo puede eliminar credenciales que no estén asociadas a un entorno de trabajo.



No se pueden eliminar las credenciales de un perfil de instancia asociado a una instancia de conector.

### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Eliminar credenciales**.
3. Haga clic en **Eliminar** para confirmar.

## Credenciales de Azure

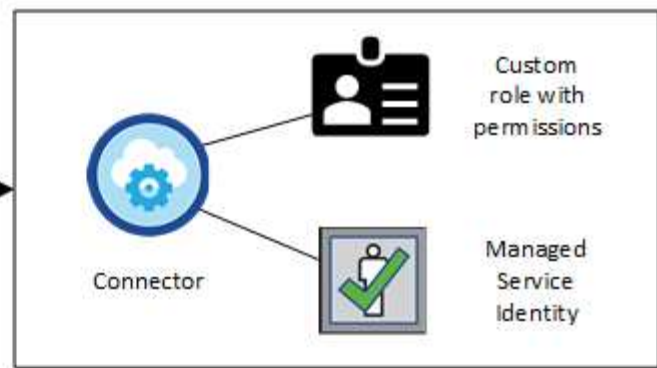
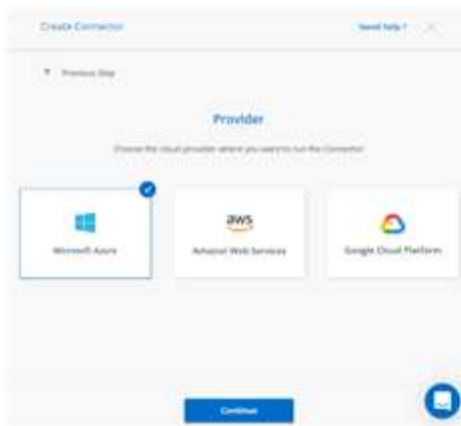
### Credenciales y permisos de Azure

BlueXP le permite elegir las credenciales de Azure que desea utilizar al poner en marcha 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 BlueXP, necesita utilizar una cuenta de Azure o una entidad de servicio con permisos para implementar la máquina virtual Connector. Los permisos necesarios se enumeran en la ["Política de implementación de conectores para Azure"](#).

Cuando BlueXP pone en marcha 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. La función proporciona a BlueXP los permisos necesarios para gestionar recursos y procesos dentro de esa suscripción a Azure. ["Revise cómo BlueXP utiliza los permisos"](#).



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

Details & Credentials			
Managed Service Ide...	OCCM QA1	<span style="color: orange;">ⓘ No subscription is associated</span>	<a href="#">Edit Credentials</a>
Credential Name	Azure Subscription	Marketplace Subscription	

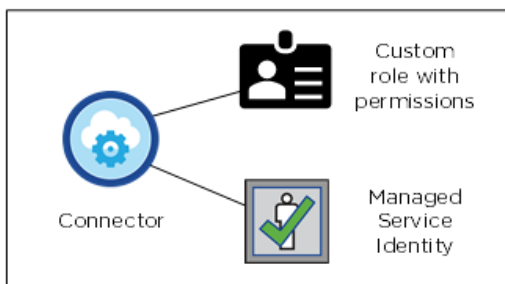
### Suscripciones adicionales de Azure para una identidad gestionada

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"](#).

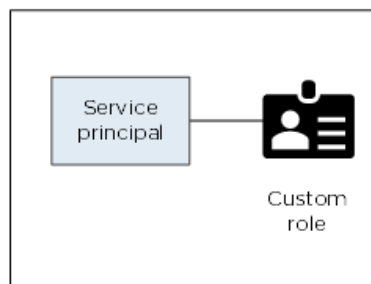
### Credenciales adicionales de Azure

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:

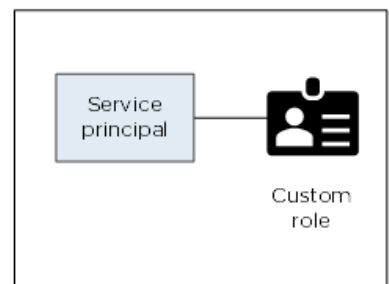
Initial Azure account



Second account



Third account

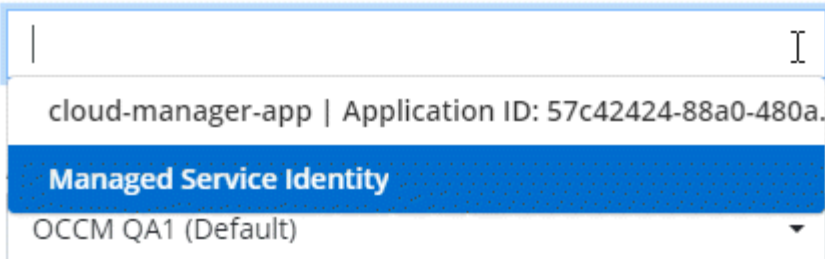


Entonces lo haría ["Agregue las credenciales de cuenta a BlueXP"](#) Proporcionando detalles acerca del director de servicio de AD.

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

## Edit Account & Add Subscription

### Credentials



The screenshot shows a web interface with a header 'Edit Account & Add Subscription'. Below it is a section titled 'Credentials'. Inside this section is a dropdown menu. The dropdown is open, showing several options. The top option is 'cloud-manager-app | Application ID: 57c42424-88a0-480a...'. Below it is a blue bar with the text 'Managed Service Identity'. At the bottom of the dropdown is 'OCCM QA1 (Default)' with a small downward arrow.

### ¿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 BlueXP. 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.

## Gestione credenciales y suscripciones de Azure para BlueXP

Al crear un sistema de Cloud Volumes ONTAP, tiene que seleccionar las credenciales de Azure para utilizarlas con ese sistema. Si utiliza licencias de pago por uso, también tendrá que elegir una suscripción a Marketplace. Siga los pasos que se indican en esta página si necesita utilizar varias credenciales de Azure o varias suscripciones a Azure Marketplace para Cloud Volumes ONTAP.

Hay dos formas de añadir credenciales y suscripciones de Azure adicionales en BlueXP.

1. Asocie las suscripciones adicionales de Azure a la identidad gestionada de Azure.
2. Si desea implementar Cloud Volumes ONTAP con diferentes credenciales de Azure, conceda permisos de Azure con un servicio principal y añada sus credenciales a BlueXP.

### Asociar suscripciones de Azure adicionales a una identidad administrada

BlueXP le permite elegir las credenciales de Azure y la suscripción a 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" Al desplegar un conector desde BlueXP. Cuando implementó el conector, BlueXP creó la función de operador BlueXP y la 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 BlueXP**.
4. Repita estos pasos para suscripciones adicionales.

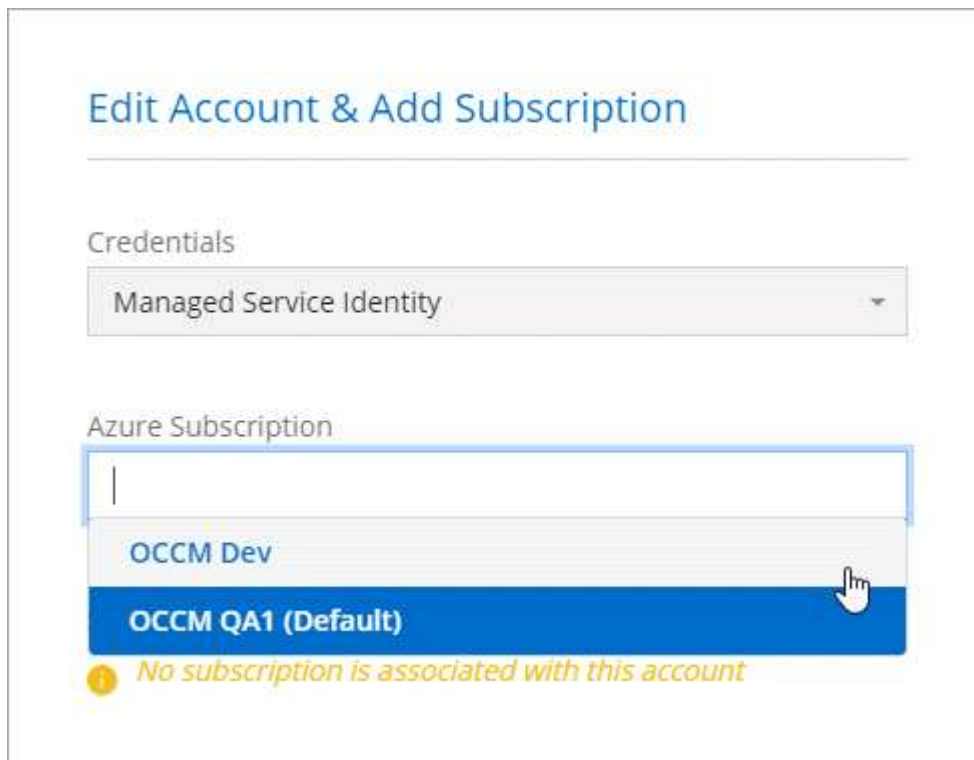


BlueXP Operator es el nombre predeterminado que se proporciona en la directiva Connector. Si seleccionó otro nombre para el rol, seleccione ese nombre.

- 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**.

### Resultado

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



## Adición de credenciales de Azure adicionales a BlueXP

Al implementar un conector desde BlueXP, BlueXP habilita una identidad administrada asignada por el sistema en la máquina virtual que tiene los permisos necesarios. BlueXP selecciona estas credenciales de Azure de forma predeterminada al crear un entorno de trabajo nuevo para Cloud Volumes ONTAP.



No se agrega un conjunto inicial de credenciales si instaló manualmente el software Connector en un sistema existente. ["Obtenga más información acerca de credenciales y permisos de Azure"](#).

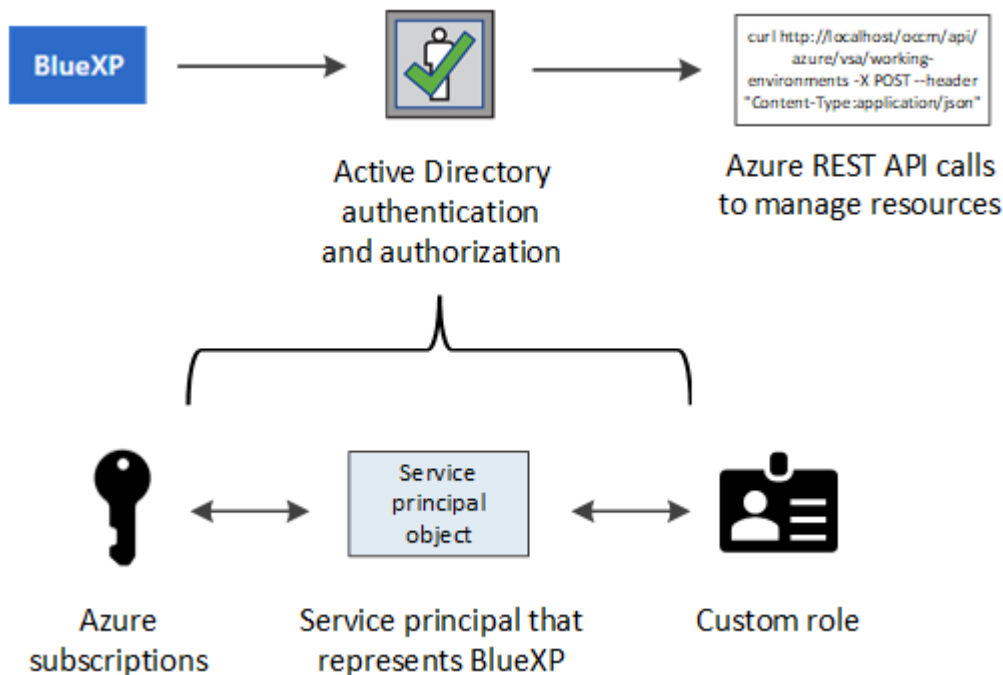
Si desea implementar Cloud Volumes ONTAP con credenciales de *diferente* Azure, debe conceder los permisos necesarios para crear y configurar un director de servicio en Azure Active Directory para cada cuenta de Azure. A continuación, puede agregar las nuevas credenciales a BlueXP.

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

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

### Acerca de esta tarea

La siguiente imagen muestra cómo BlueXP obtiene permisos para realizar operaciones en Azure. Un objeto principal de servicio, que está vinculado a una o más suscripciones de Azure, representa BlueXP 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

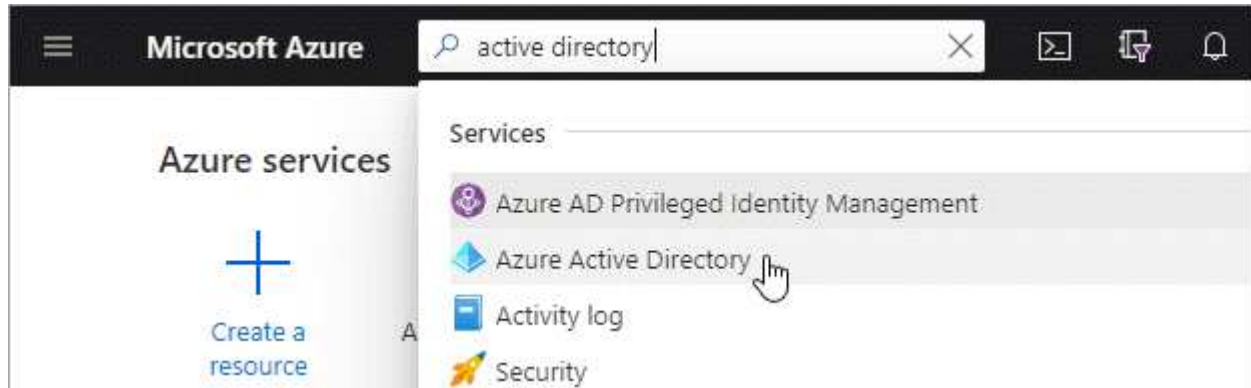
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que BlueXP pueda usar para el control de acceso basado en roles.

### 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 BlueXP).
  - **Redirigir URI:** Puede dejar este campo en blanco.
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 de operador "BlueXP Operator" personalizado para que BlueXP tenga permisos en Azure.

### Pasos

1. Crear un rol personalizado:
  - a. Copie el contenido de ["Permisos de función personalizada para el conector"](#) Y guárdelos en un archivo JSON.
  - 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.

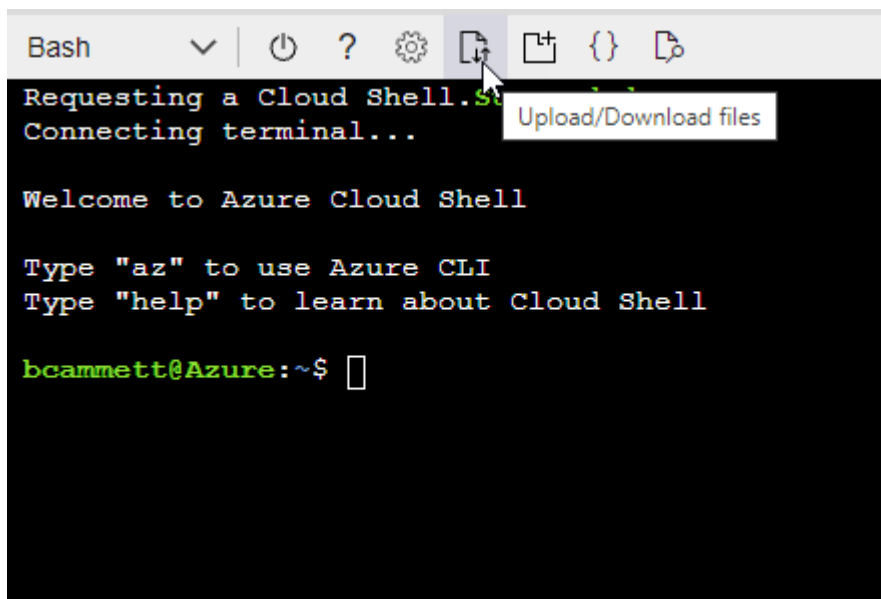
## ejemplo

```
"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.

En los pasos siguientes se describe cómo crear la función mediante Bash en Azure Cloud Shell.

- Comenzar "Shell de cloud de Azure" Y seleccione el entorno Bash.
- Cargue el archivo JSON.



- Use la interfaz de línea de comandos de Azure para crear el rol personalizado:

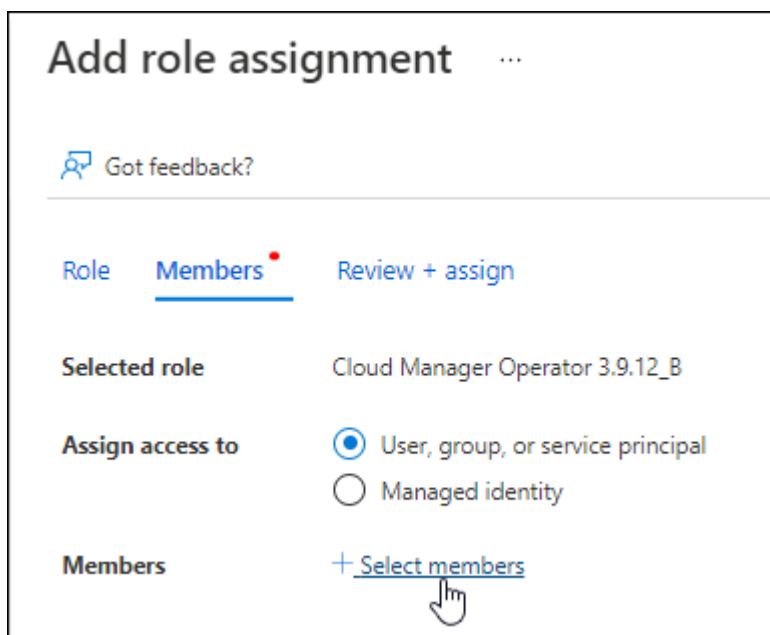
```
az role definition create --role-definition Connector_Policy.json
```

Ahora debe tener una función personalizada denominada operador BlueXP que puede asignar a la máquina virtual Connector.

## 2. Asigne la aplicación al rol:

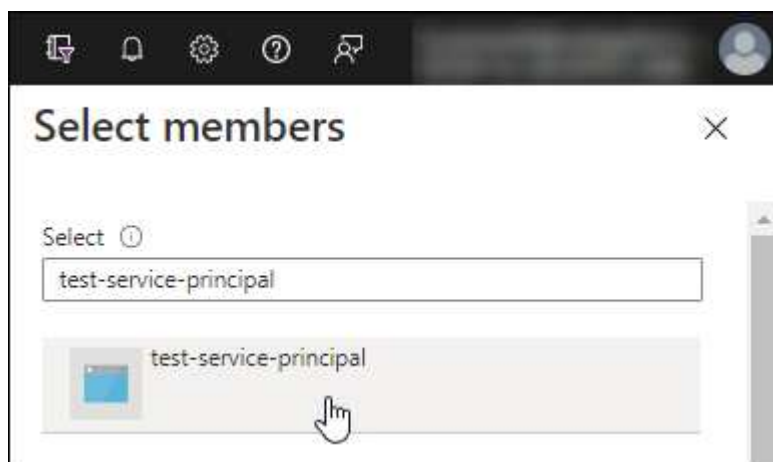
- a. En el portal de Azure, abra el servicio **Suscripciones**.
- b. Seleccione la suscripción.
- c. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
- d. En la ficha **rol**, seleccione el rol **operador BlueXP** y haga clic en **Siguiente**.
- e. En la ficha **Miembros**, realice los siguientes pasos:
  - Mantener seleccionado **Usuario, grupo o principal de servicio**.

- Haga clic en **Seleccionar miembros**.



- Busque el nombre de la aplicación.

Veamos un ejemplo:



- Seleccione la aplicación y haga clic en **Seleccionar**.
  - Haga clic en **Siguiente**.
- f. Haga clic en **revisar + asignar**.

El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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

**Microsoft Graph**  
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](#)

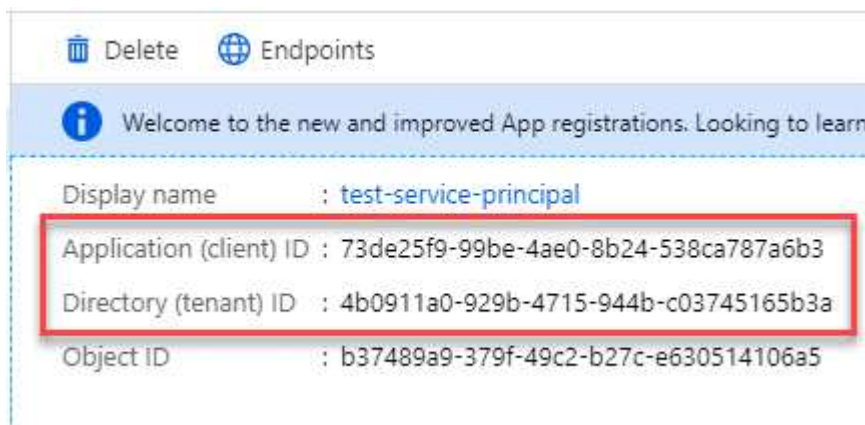
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

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

Al agregar la cuenta de Azure a BlueXP, debe proporcionar el ID de la aplicación (cliente) y el ID de directorio (inquilino) para la aplicación. BlueXP utiliza los identificadores 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

Necesita crear un secreto de cliente y, a continuación, proporcionar BlueXP con el valor del secreto para que BlueXP pueda utilizarlo para autenticar con Azure AD.

### 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**.

- Proporcione una descripción del secreto y una duración.
- Haga clic en **Agregar**.
- 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	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	Copy to clipboard

### 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 BlueXP cuando agrega una cuenta de Azure.

### Agregar las credenciales a BlueXP

Después de proporcionar una cuenta de Azure con los permisos necesarios, puede añadir las credenciales para esa cuenta a BlueXP. Completar este paso le permite iniciar Cloud Volumes ONTAP con diferentes credenciales de Azure.

### Antes de empezar

Si acaba de crear estas credenciales en su proveedor de cloud, es posible que transcurran unos minutos hasta que estén disponibles para su uso. Espere unos minutos antes de agregar las credenciales a BlueXP.

### Lo que necesitará

Debe crear un conector para poder cambiar la configuración de BlueXP. ["Vea cómo"](#).

### Pasos

- En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.



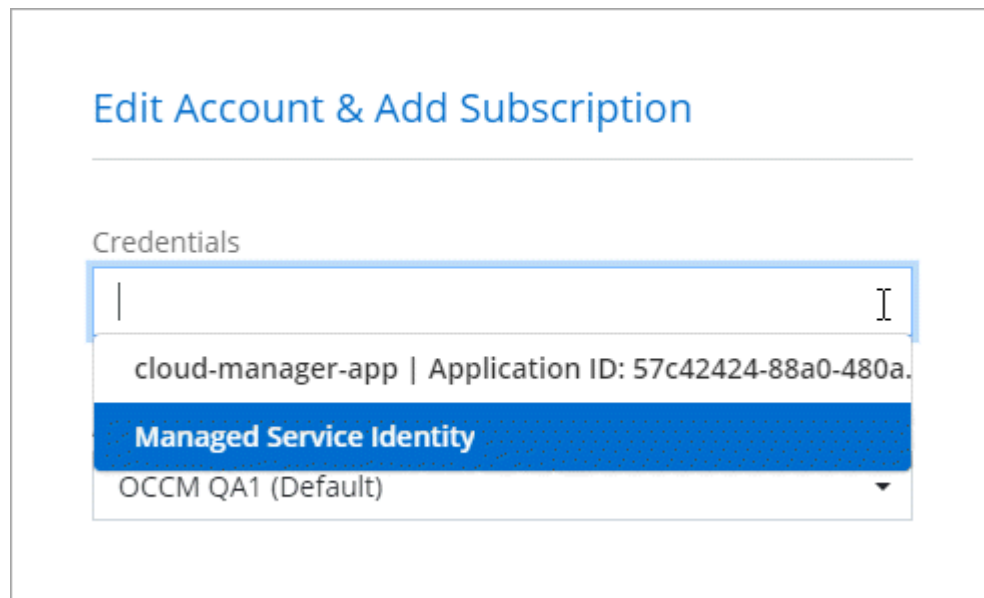
- Haga clic en **Agregar credenciales** y siga los pasos del asistente.
  - Ubicación de credenciales:** Seleccione **Microsoft Azure > conector**.
  - Definir credenciales:** Introduzca información acerca del principal de servicio de Azure Active Directory que otorga los permisos necesarios:
    - ID 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](#).
  - Suscripción al mercado:** Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

Para pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO), estas credenciales de Azure deben estar asociadas con una suscripción a Azure Marketplace.

d. **Revisión:** Confirme los detalles acerca de las nuevas credenciales y 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](#)"



## Gestionar las credenciales existentes

Gestione las credenciales de Azure que ya ha agregado a BlueXP asociando una suscripción de Marketplace, editando credenciales y suprimiéndolas.

## Asociación de una suscripción de Azure Marketplace a credenciales

Después de añadir sus credenciales de Azure a BlueXP, 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 situaciones en las que puede asociar una suscripción a Azure Marketplace después de haber añadido las credenciales a BlueXP:

- No asoció una suscripción cuando agregó inicialmente las credenciales a BlueXP.
- Desea sustituir una suscripción existente de Azure Marketplace por una nueva suscripción.

## Lo que necesitará

Debe crear un conector para poder cambiar la configuración de BlueXP. "[Vea cómo](#)".

## Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Suscripción asociada**.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y haga clic en **asociado**.
4. Para asociar las credenciales con una nueva suscripción, haga clic en **Agregar suscripción > continuar** y siga los pasos de Azure Marketplace:
  - a. Si se le solicita, inicie sesión en su cuenta de Azure.
  - b. Haga clic en **Suscribirse**.
  - c. Rellene el formulario y haga clic en **Suscribirse**.
  - d. Una vez completado el proceso de suscripción, haga clic en **Configurar cuenta ahora**.

Se le redirigirá al sitio web de BlueXP.

- e. Desde la página **asignación de suscripción**:

- Seleccione las cuentas de NetApp a las que desea asociar esta suscripción.
- En el campo **sustituir suscripción existente**, elija si desea sustituir automáticamente la suscripción existente para una cuenta con esta nueva suscripción.

BlueXP reemplaza la suscripción existente para todas las credenciales de la cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Haga clic en **Guardar**.

En el siguiente vídeo se muestran los pasos para suscribirse desde Azure Marketplace:

► [https://docs.netapp.com/es-es/cloud-manager-setup-admin//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/es-es/cloud-manager-setup-admin//media/video_subscribing_azure.mp4)



(video)

### Editar credenciales

Edite sus credenciales de Azure en BlueXP modificando los detalles acerca de sus credenciales de servicio de Azure. Por ejemplo, es posible que necesite actualizar el secreto de cliente si se creó un nuevo secreto para la aplicación principal de servicios.

#### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Editar credenciales**.
3. Realice los cambios necesarios y, a continuación, haga clic en **aplicar**.

### Eliminación de credenciales

Si ya no necesita un conjunto de credenciales, puede eliminarlas de BlueXP. Sólo puede eliminar credenciales que no estén asociadas a un entorno de trabajo.

#### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Eliminar credenciales**.
3. Haga clic en **Eliminar** para confirmar.

## Credenciales de Google Cloud

### Proyectos, permisos y cuentas de Google Cloud

Una cuenta de servicio proporciona a BlueXP permisos para implementar y administrar sistemas Cloud Volumes ONTAP que se encuentran en el mismo proyecto que el conector o en proyectos diferentes.

#### Proyecto y permisos para BlueXP

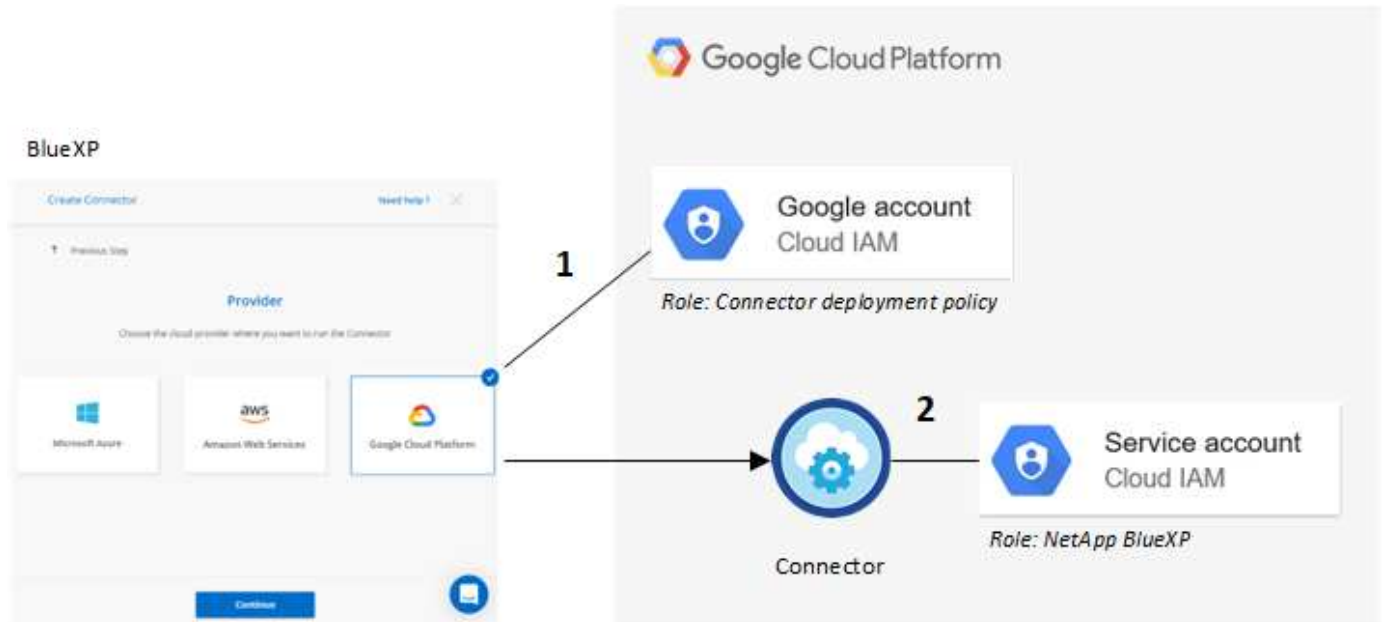
Antes de poder poner en marcha Cloud Volumes ONTAP en Google Cloud, primero debe poner en marcha un conector en un proyecto de Google Cloud. El conector no puede ejecutarse en sus instalaciones ni en un proveedor de cloud diferente.

Deben existir dos conjuntos de permisos antes de desplegar un conector directamente desde BlueXP:

1. Debe implementar un conector utilizando una cuenta de Google que tenga permisos para iniciar la instancia de Connector VM desde BlueXP.
2. Al desplegar el conector, se le pedirá que seleccione un "cuenta de servicio" Para la instancia de máquina virtual. BlueXP obtiene permisos de la cuenta de servicio para crear y administrar sistemas 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](#)"
- "[Descubra cómo implementar Cloud Volumes ONTAP en GCP y seleccione un proyecto](#)"

## Gestión de credenciales y suscripciones de Google Cloud para BlueXP

Puede gestionar las credenciales asociadas a la instancia de Connector VM.

### Asociación de una suscripción a Marketplace con credenciales de Google Cloud

Al implementar un conector en Google Cloud, BlueXP crea un conjunto predeterminado de credenciales asociadas a la instancia de Connector VM. Estas son las credenciales que BlueXP utiliza para implementar 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 parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **credenciales**.
2. Haga clic en el menú de acción para obtener un conjunto de credenciales y, a continuación, seleccione **Suscripción asociada**.



3. Para asociar las credenciales a una suscripción existente, seleccione un proyecto de Google Cloud y una suscripción en la lista desplegable y, a continuación, haga clic en **asociado**.

Google Cloud Project

OCCM-Dev ▼

Subscription

● GCP subscription for staging ▼

---

[+ Add Subscription](#)

4. Si aún no tiene una suscripción, haga clic en **Agregar suscripción > continuar** y siga los pasos de Google Cloud Marketplace.



Antes de completar los siguientes pasos, asegúrese de que tiene privilegios de administrador de facturación en su cuenta de Google Cloud así como un inicio de sesión de BlueXP.

- a. Cuando se le haya redirigido a ["Página de BlueXP de NetApp en Google Cloud Marketplace"](#), asegúrese de seleccionar el proyecto correcto en el menú de navegación superior.

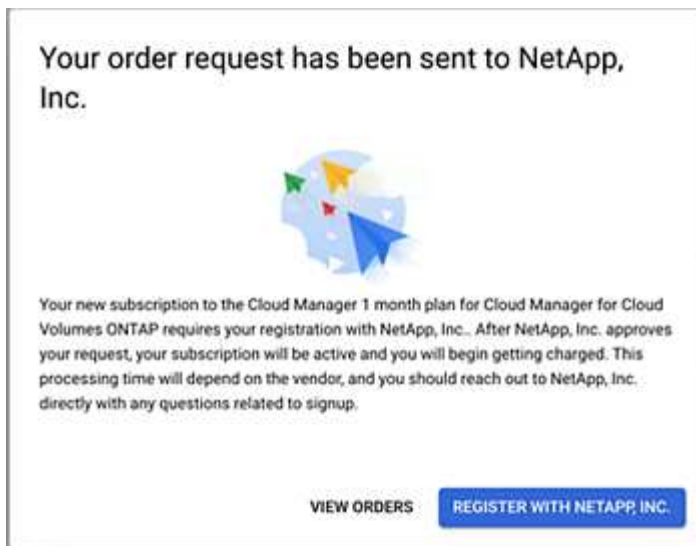
The screenshot shows the 'Product details' page for NetApp BlueXP on the Google Cloud platform. At the top, there's a navigation bar with the Google Cloud logo and a dropdown menu showing 'netapp.com'. Below this, a back arrow and the text 'Product details' are visible. The main content area features the NetApp logo, the product name 'NetApp BlueXP', and a link to 'NetApp, Inc.'. A description states: 'BlueXP lets you build, protect, and govern your hybrid multicloud data estate.' A prominent blue 'SUBSCRIBE' button is centered. Below the button, there are four tabs: 'OVERVIEW' (which is selected and underlined), 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. The 'Overview' section contains two paragraphs of text describing the product's capabilities. To the right of the overview, there is a section titled 'Additional details' which includes the product type ('SaaS & APIs'), the last update date ('12/19/22'), and a category list ('Analytics, Developer tools, Storage').

- b. Haga clic en **Suscribirse**.
- c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.
- d. Haga clic en **Suscribirse**.

Este paso envía la solicitud de transferencia a NetApp.

- e. En el cuadro de diálogo emergente, haga clic en **Registrar con NetApp, Inc.**

Este paso debe completarse para vincular la suscripción a Google Cloud a su cuenta de NetApp. El proceso de vinculación de una suscripción no está completo hasta que se le redirigirá de esta página y, a continuación, inicie sesión en BlueXP.



f. Siga los pasos de la página **asignación de suscripción**:



Si alguien de su organización ya se ha suscrito a la suscripción de NetApp BlueXP desde su cuenta de facturación, se le redirigirá a "[La página Cloud Volumes ONTAP en el sitio Web de BlueXP](#)" en su lugar. Si esto no se realiza de forma inesperada, póngase en contacto con el equipo de ventas de NetApp. Google sólo activa una suscripción por cuenta de facturación de Google.

- Seleccione las cuentas de NetApp a las que desea asociar esta suscripción.
- En el campo **sustituir suscripción existente**, elija si desea sustituir automáticamente la suscripción existente para una cuenta con esta nueva suscripción.

BlueXP reemplaza la suscripción existente para todas las credenciales de la cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Haga clic en **Guardar**.

En el siguiente vídeo se muestran los pasos para suscribirse desde Google Cloud Marketplace:

► <https://docs.netapp.com/es-es/cloud-manager-setup-admin//media/video-subscribing-google-cloud.mp4>


(video)

- a. Una vez completado este proceso, vuelva a la página credenciales de BlueXP y seleccione esta nueva suscripción.


Google Cloud Project

OCCM-Dev

Subscription



GCP subscription for staging



Add Subscription

## Solución de problemas del proceso de suscripción de Marketplace

A veces, suscribirse a Cloud Volumes ONTAP a través de Google Cloud Marketplace se puede fragmentar debido a permisos incorrectos o no haber seguido accidentalmente la redirección al sitio web de BlueXP. Si esto sucede, siga estos pasos para completar el proceso de suscripción.

### Pasos

1. Desplácese hasta la "[Página de BlueXP de NetApp en Google Cloud Marketplace](#)" para comprobar el estado del pedido. Si la página indica **Administrar en Proveedor**, desplácese hacia abajo y haga clic en **gestionar pedidos**.

### Pricing



The product was purchased on 12/9/20.

[MANAGE ORDERS](#)

- Si el pedido muestra una Marca de verificación verde y esto es inesperado, puede que ya se suscriban otras personas de la organización que utilicen la misma cuenta de facturación. Si esto no se realiza lo esperado o necesita los detalles de esta suscripción, póngase en contacto con su equipo de ventas de NetApp.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	2eebbc... 	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	

- Si el pedido muestra un reloj y el estado **pendiente**, vuelva a la página de mercado y seleccione **Administrar en proveedor** para completar el proceso como se ha documentado anteriormente.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
🕒	d56c66... 📄	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	⋮

## Gestione cuentas del sitio de soporte de NetApp en BlueXP

Proporcione las credenciales para que sus cuentas del sitio de soporte de NetApp (NSS) se registren para admitir, habilitar flujos de trabajo clave para Cloud Volumes ONTAP, etc.

### Descripción general

BlueXP admite la asociación de una cuenta NSS a cada usuario de BlueXP y la asociación de una o más cuentas de NSS a su cuenta de BlueXP.

### Credenciales de NSS por usuario de BlueXP

Se requieren sus credenciales de NSS individuales para acceder a su cuenta de Digital Advisor y gestionar los casos de soporte a través de BlueXP. Estas credenciales sólo son visibles para la persona que inicia sesión en BlueXP. Las credenciales se pueden eliminar y actualizar según sea necesario.

[Aprenda a administrar credenciales de NSS por usuario de BlueXP.](#)

### Credenciales de NSS para su cuenta de BlueXP

Se requiere la asociación de las credenciales del sitio de soporte de NetApp con el ID de cuenta de BlueXP específico para habilitar las siguientes tareas en BlueXP:

- Registro para recibir soporte
- Creación de casos de soporte
- Puesta en marcha de Cloud Volumes ONTAP cuando usted traiga su propia licencia (BYOL)

Es necesario proporcionar su cuenta NSS para que BlueXP pueda cargar su clave de licencia y activar la suscripción para el plazo que adquirió. Esto incluye actualizaciones automáticas para renovaciones de términos.

- Registro de sistemas Cloud Volumes ONTAP de pago por uso

Se requiere que proporcione su cuenta de NSS para activar el soporte de su sistema y obtener acceso a los recursos de soporte técnico de NetApp.

- Actualizar el software Cloud Volumes ONTAP a la versión más reciente

Estas credenciales están asociadas a su ID de cuenta de BlueXP específico. Los usuarios que pertenecen a la cuenta BlueXP pueden acceder a estas credenciales desde **Soporte > Gestión NSS**.

[Aprenda a administrar credenciales de NSS para su cuenta de BlueXP.](#)

### Administre las credenciales de NSS para su inicio de sesión de BlueXP

Las credenciales de NSS asociadas con el inicio de sesión de BlueXP permiten acceder a Digital Advisor y

capacidades de gestión de casos.

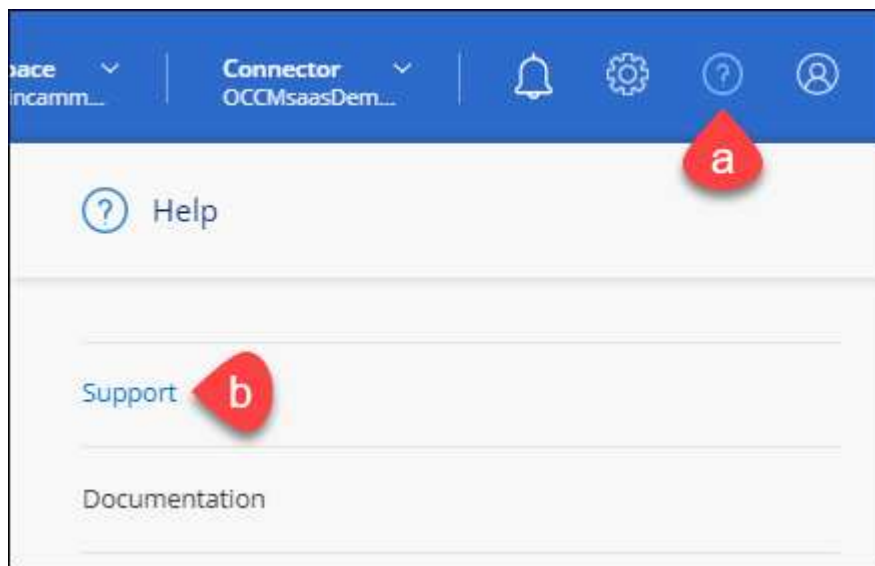
- Al acceder a Digital Advisor en BlueXP, se le pedirá que inicie sesión en Digital Advisor introduciendo sus credenciales de NSS. Después de introducir sus credenciales de NSS, verá esta cuenta de NSS que aparece en la parte superior de la página NSS Management. A continuación, puede gestionar esas credenciales según sea necesario.
- Al acceder a **Soporte > Administración de casos**, se le pedirá que introduzca sus credenciales de NSS, si aún no lo ha hecho. En esta página se muestran los casos de soporte asociados con su cuenta de NSS y con su empresa.

Tenga en cuenta lo siguiente acerca de esta cuenta de NSS:

- La cuenta se gestiona en el nivel de usuario, lo que significa que otros usuarios que inician sesión no la pueden ver.
- La cuenta no se puede utilizar con ninguna otra función de BlueXP: No con la creación de Cloud Volumes ONTAP, la licencia ni la creación de casos de soporte.
- Sólo puede haber una cuenta NSS asociada con Digital Advisor y gestión de casos, por usuario.

### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.



2. Haga clic en **NSS Management**.
3. En **sus credenciales de NSS**, haga clic en **Acción** y elija cualquiera de las siguientes opciones:
  - **Usuario de NSS asociado:** Añadir credenciales para una cuenta del sitio de soporte de NetApp.
  - **Actualizar las credenciales existentes:** Actualizar las credenciales de su cuenta del sitio de soporte de NetApp.
  - **Eliminar:** Elimina la cuenta asociada a tu cuenta de usuario de BlueXP.

### Resultado

BlueXP actualiza sus credenciales de NSS. Los cambios se reflejarán al acceder a Digital Advisor o a la página Administración de casos.



## Administre las credenciales de NSS para su cuenta de BlueXP

Gestione las credenciales de NSS asociadas con su cuenta de BlueXP para que pueda registrarse en la asistencia técnica, crear casos de soporte y habilitar flujos de trabajo clave para Cloud Volumes ONTAP.

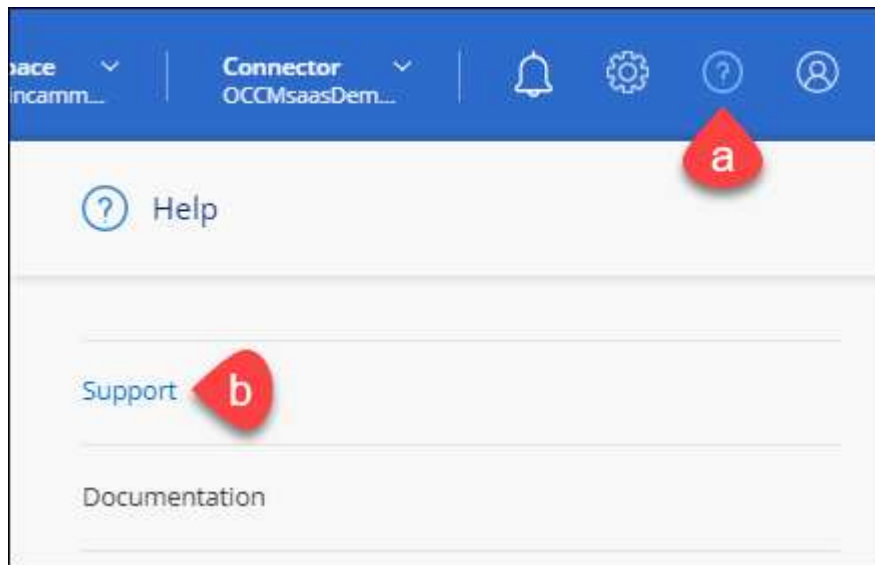
### Añada una cuenta de NSS

La consola de soporte le permite añadir y gestionar sus cuentas de la página de soporte de NetApp para utilizarlas con BlueXP a nivel de cuenta de BlueXP.

- Si tiene una cuenta de nivel de cliente, puede añadir una o varias cuentas de NSS.
- Si tiene una cuenta de partner o distribuidor, puede añadir una o varias cuentas de NSS, pero no se podrán añadir junto con las cuentas de nivel de cliente.

### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.



2. Haga clic en **Administración de NSS > Agregar cuenta de NSS**.
3. Cuando se le pregunte, haga clic en **continuar** para que se le redirija a una página de inicio de sesión de Microsoft.

NetApp utiliza Microsoft Azure Active Directory como proveedor de identidades para servicios de autenticación específicos para soporte y licencias.

4. En la página de inicio de sesión, proporcione su dirección de correo electrónico registrada en el sitio de soporte de NetApp y contraseña para realizar el proceso de autenticación.

Estas acciones permiten a BlueXP utilizar su cuenta NSS para cosas como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.

Tenga en cuenta lo siguiente:


- La cuenta NSS debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal). Puede tener varias cuentas de NSS en el nivel del cliente.
- Sólo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de partner. Si intenta agregar cuentas de NSS de nivel de cliente y existe una cuenta de nivel de partner, obtendrá el siguiente


mensaje de error:

"El tipo de cliente NSS no está permitido para esta cuenta, ya que ya hay usuarios NSS de tipo diferente."

Lo mismo sucede si tiene cuentas de NSS de nivel de cliente preexistentes e intenta añadir una cuenta de nivel de partner.

- Después de iniciar sesión correctamente, NetApp almacenará el nombre de usuario de NSS.

Se trata de un ID generado por el sistema que se asigna a su correo electrónico. En la página **NSS Management**, puede mostrar su correo electrónico desde  de windows

- Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en la  de windows

Con esta opción se le solicita que vuelva a iniciar sesión. Tenga en cuenta que el token de estas cuentas caduca después de 90 días. Se enviará una notificación para avisarle de ello.

## El futuro

Los usuarios ahora pueden seleccionar la cuenta al crear nuevos sistemas de Cloud Volumes ONTAP, al registrar los sistemas de Cloud Volumes ONTAP existentes y al registrarse para obtener soporte.

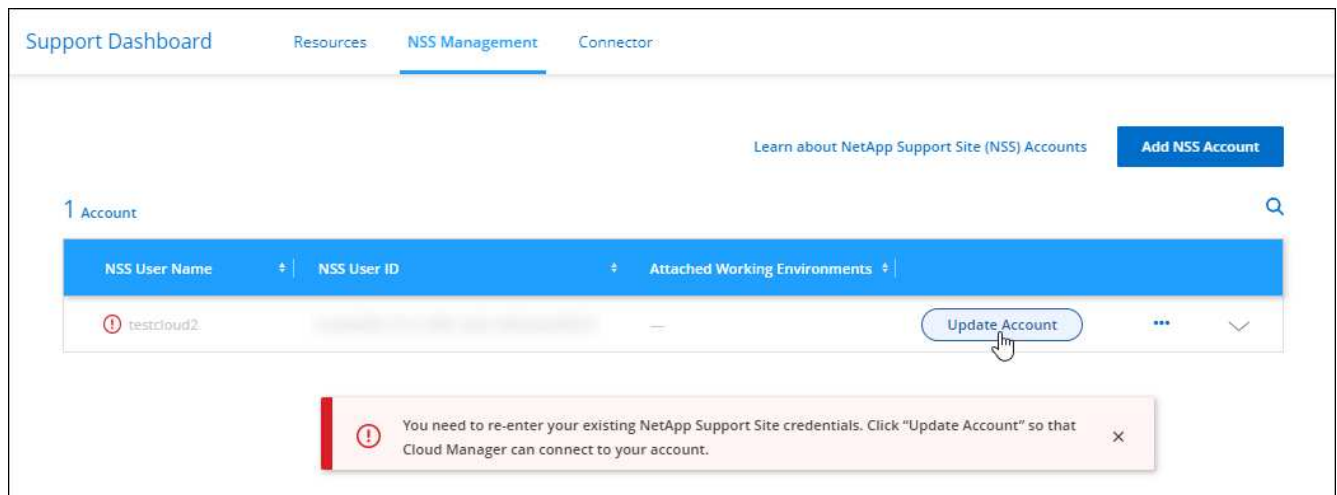
- ["Inicio de Cloud Volumes ONTAP en AWS"](#)
- ["Inicio de Cloud Volumes ONTAP en Azure"](#)
- ["Lanzamiento de Cloud Volumes ONTAP en GCP"](#)
- ["Registro de sistemas de pago por uso"](#)

## Actualice una cuenta de NSS para el nuevo método de autenticación

A partir de noviembre de 2021, NetApp ahora utiliza Microsoft Azure Active Directory como proveedor de identidades para servicios de autenticación específicos para soporte y licencias. Como resultado de esta actualización, BlueXP le solicitará que actualice las credenciales de cualquier cuenta existente que haya agregado previamente.

## Pasos

1. Si aún no lo ha hecho, ["Cree una cuenta B2C de Microsoft Azure Active Directory que estará vinculada a su cuenta actual de NetApp"](#).
2. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.
3. Haga clic en **NSS Management**.
4. Para obtener la cuenta NSS que desea actualizar, haga clic en **Actualizar cuenta**.



5. Cuando se le pregunte, haga clic en **continuar** para que se le redirija a una página de inicio de sesión de Microsoft.

NetApp utiliza Microsoft Azure Active Directory como proveedor de identidades para servicios de autenticación específicos para soporte y licencias.

6. En la página de inicio de sesión, proporcione su dirección de correo electrónico registrada en el sitio de soporte de NetApp y contraseña para realizar el proceso de autenticación.

Una vez completado el proceso, la cuenta que ha actualizado debería aparecer ahora como una cuenta *new* en la tabla. La versión *older* de la cuenta sigue apareciendo en la tabla, junto con cualquier asociación de entorno de trabajo existente.

7. Si los entornos de trabajo existentes de Cloud Volumes ONTAP están asociados a la versión anterior de la cuenta, siga los pasos que se indican a continuación [Adjunte esos entornos de trabajo a una cuenta de NSS diferente](#).
8. Vaya a la versión anterior de la cuenta NSS, haga clic en **...** Y, a continuación, seleccione **Eliminar**.

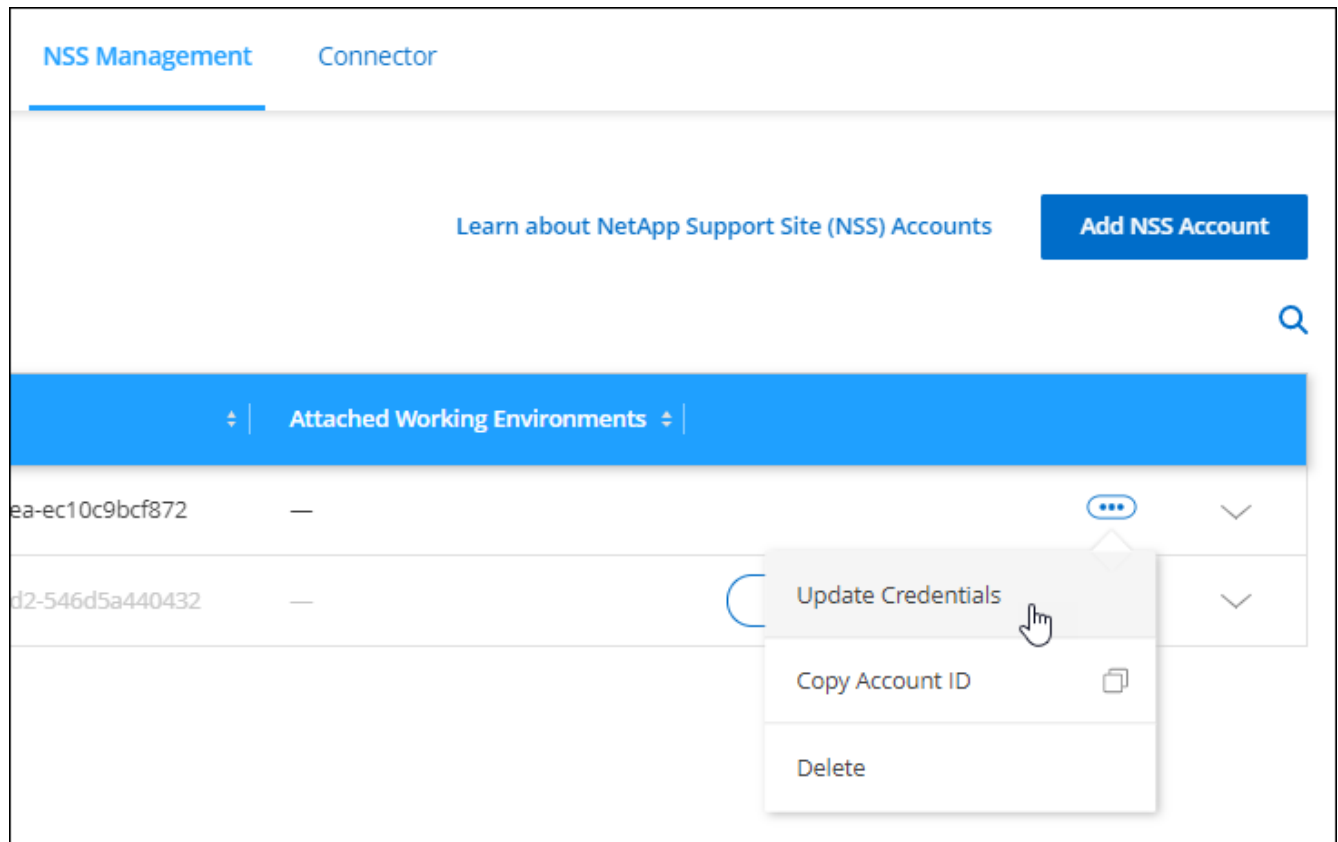
### Actualice las credenciales de NSS

Deberá actualizar las credenciales de sus cuentas de NSS en BlueXP cuando se produzca una de las siguientes situaciones:

- Las credenciales de la cuenta se cambian
- El token de actualización asociado con su cuenta caduca después de 3 meses

### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.
2. Haga clic en **NSS Management**.
3. Para la cuenta de NSS que desea actualizar, haga clic en **...** Y, a continuación, seleccione **Actualizar credenciales**.



4. Cuando se le pregunte, haga clic en **continuar** para que se le redirija a una página de inicio de sesión de Microsoft.

NetApp utiliza Microsoft Azure Active Directory como proveedor de identidades para servicios de autenticación específicos para soporte y licencias.

5. En la página de inicio de sesión, proporcione su dirección de correo electrónico registrada en el sitio de soporte de NetApp y contraseña para realizar el proceso de autenticación.

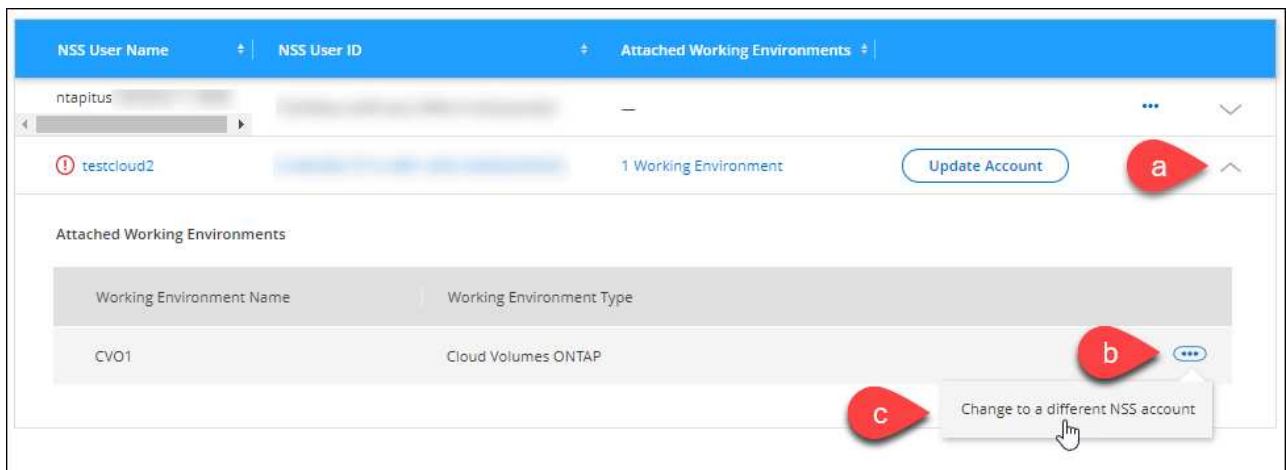
### Adjunte un entorno de trabajo a una cuenta de NSS diferente

Si su organización tiene varias cuentas del sitio de soporte de NetApp, puede cambiar qué cuenta está asociada a un sistema Cloud Volumes ONTAP.

Esta función solo es compatible con cuentas de NSS que se han configurado para usar Microsoft Azure AD adoptado por NetApp para la gestión de identidades. Para poder utilizar esta función, necesita hacer clic en **Agregar cuenta de NSS** o **Actualizar cuenta**.

#### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.
2. Haga clic en **NSS Management**.
3. Complete los siguientes pasos para cambiar la cuenta de NSS:
  - a. Expanda la fila de la cuenta del sitio de soporte de NetApp con la que está asociado actualmente el entorno de trabajo.
  - b. Para el entorno de trabajo para el que desea cambiar la asociación, haga clic en **...**
  - c. Seleccione **Cambiar a una cuenta de NSS diferente**.



d. Seleccione la cuenta y haga clic en **Guardar**.

### Muestra la dirección de correo electrónico de una cuenta de NSS

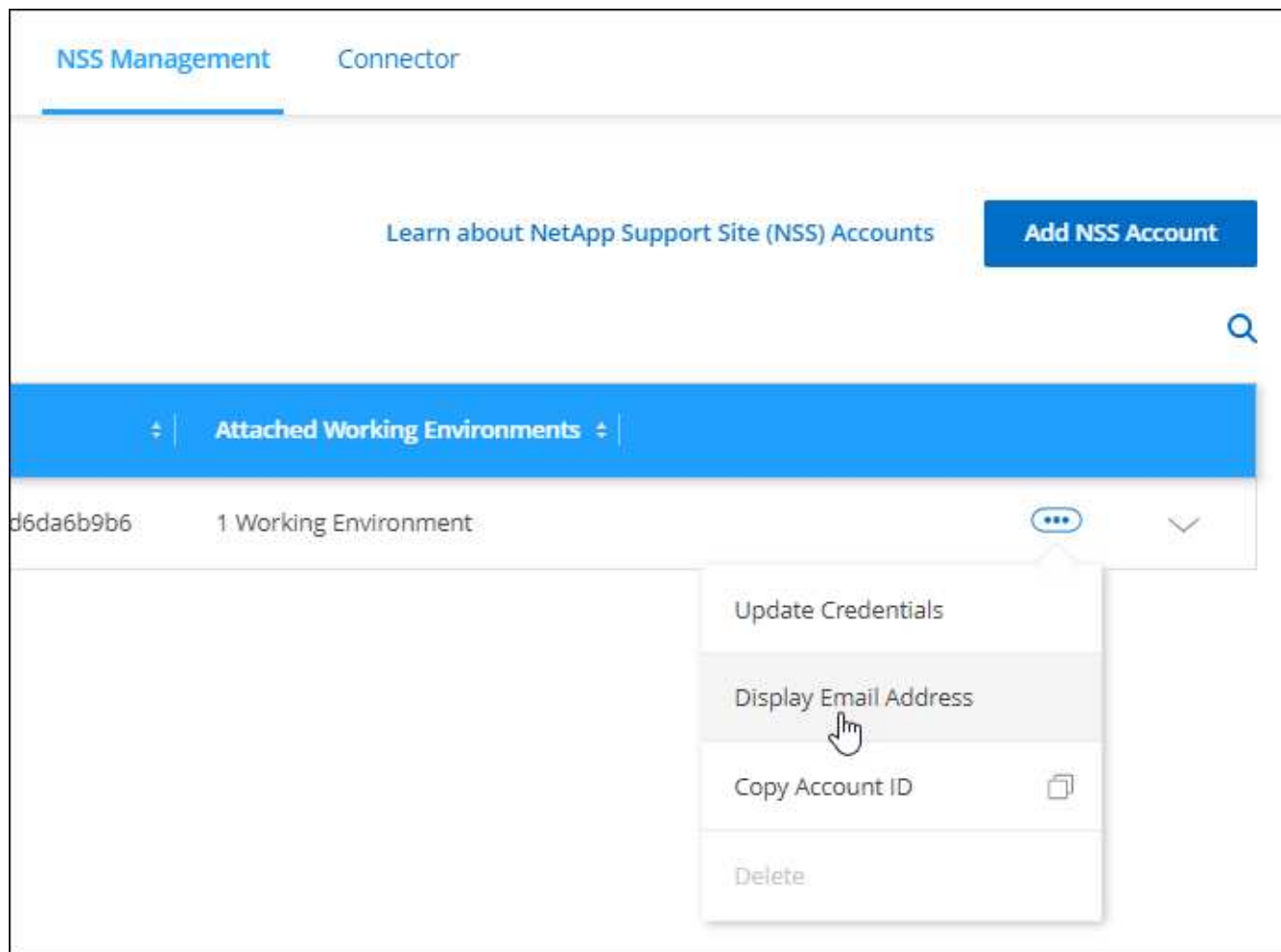
Ahora que las cuentas del sitio de soporte de NetApp usan Microsoft Azure Active Directory para los servicios de autenticación, el nombre de usuario de NSS que aparece en BlueXP suele ser un identificador generado por Azure AD. Como resultado, es posible que no conozca inmediatamente la dirección de correo electrónico asociada a esa cuenta. Pero BlueXP tiene la opción de mostrarle la dirección de correo electrónico asociada.



Cuando vaya a la página NSS Management, BlueXP genera un token para cada cuenta de la tabla. Ese token incluye información acerca de la dirección de correo electrónico asociada. A continuación, el token se elimina cuando se sale de la página. La información nunca se almacena en la caché, lo que ayuda a proteger su privacidad.

### Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.
2. Haga clic en **NSS Management**.
3. Para la cuenta de NSS que desea actualizar, haga clic en **...** Y, a continuación, seleccione **Mostrar dirección de correo electrónico**.



## Resultado

BlueXP muestra el nombre de usuario del sitio de soporte de NetApp y la dirección de correo electrónico asociada. Puede utilizar el botón de copia para copiar la dirección de correo electrónico.

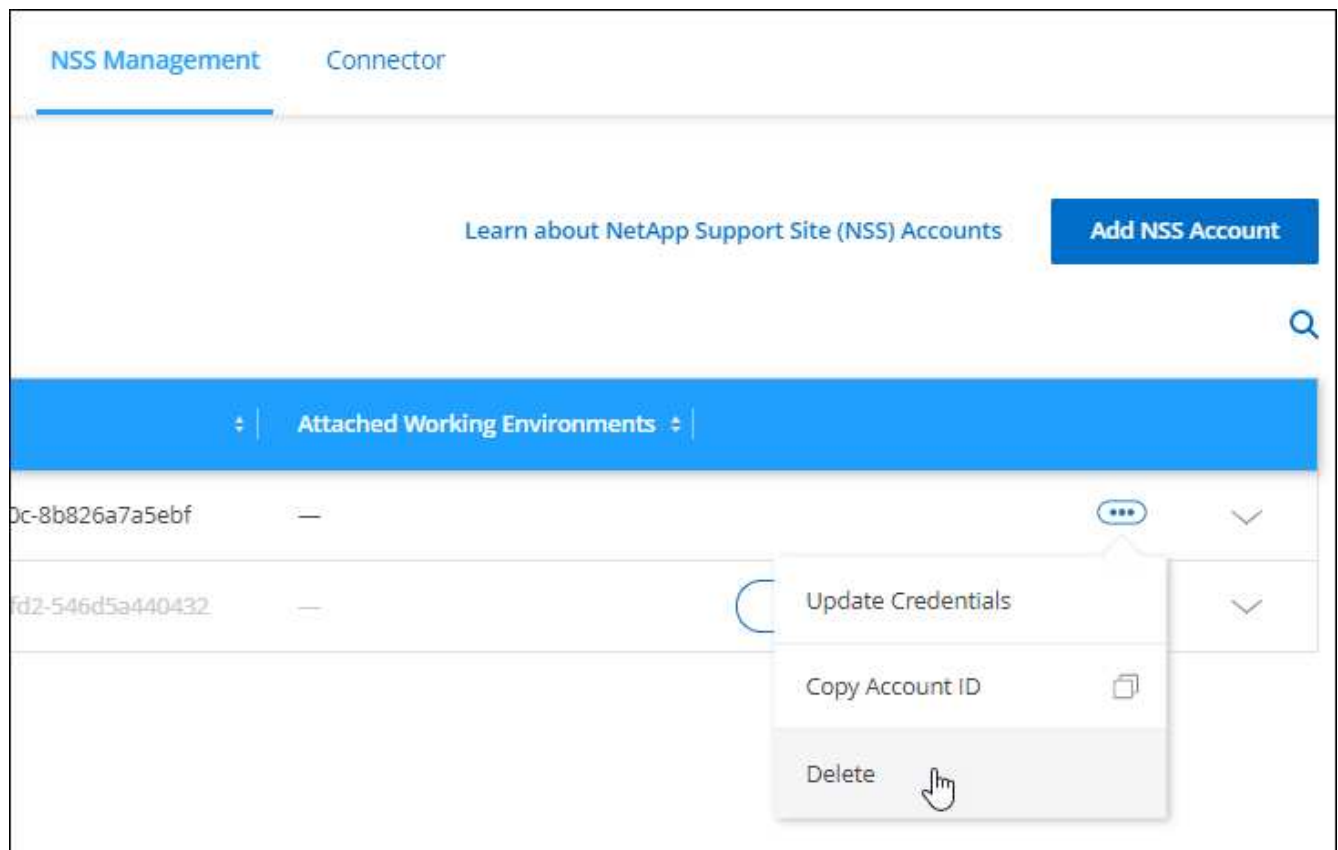
## Quite una cuenta de NSS

Elimine cualquiera de las cuentas de NSS que ya no desee utilizar con BlueXP.

Tenga en cuenta que no puede eliminar una cuenta que esté actualmente asociada a un entorno de trabajo de Cloud Volumes ONTAP. Primero tienes que hacerlo [Adjunte esos entornos de trabajo a una cuenta de NSS diferente](#).

## Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.
2. Haga clic en **NSS Management**.
3. Para la cuenta de NSS que desea eliminar, haga clic en **...** Y, a continuación, seleccione **Eliminar**.



4. Haga clic en **Eliminar** para confirmar.

## Mis oportunidades

En el lienzo, la ficha **Mis oportunidades** proporciona una ubicación centralizada para descubrir los recursos existentes que puede añadir a BlueXP para ofrecer servicios de datos y operaciones coherentes a través de su multicloud híbrido.

Actualmente, Mis oportunidades le permiten descubrir los sistemas de archivos FSX para ONTAP existentes en su cuenta de AWS.

["Aprenda a descubrir FSX para ONTAP con mis oportunidades"](#)

## Información de copyright

Copyright © 2023 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.