



Configurar y administrar BlueXP

Set up and administration

NetApp

February 20, 2023

Tabla de Contenido

Configurar y administrar BlueXP	1
Notas de la versión	2
Lo nuevo	2
Limitaciones conocidas	14
Manos a la obra	16
Más información sobre BlueXP	16
Lista de comprobación de introducción	17
Regístrese en BlueXP	21
Inicie sesión en BlueXP	22
Configure una cuenta de NetApp	23
Configure un conector	31
A continuación, ¿dónde ir	72
Administrar BlueXP	74
Cuentas de NetApp	74
Conectores	89
Gestionar suscripciones y contratos de PAYGO	118
Almacenamiento en cloud detectado	119
Credenciales de AWS	124
Credenciales de Azure	133
Credenciales de Google Cloud	146
Añadir y gestionar cuentas del sitio de soporte de NetApp en BlueXP	152
Mis oportunidades	159
Referencia	160
Permisos	160
Puertos	213
Conocimiento y apoyo	219
Regístrese para recibir soporte	219
Obtenga ayuda	223
Avisos legales	227
Derechos de autor	227
Marcas comerciales	227
Estadounidenses	227
Política de privacidad	227
Código abierto	227

Configurar y administrar BlueXP

Notas de la versión

Lo nuevo

Descubra las novedades de las funciones de administración de BlueXP (antes Cloud Manager): Cuentas de NetApp, conectores, credenciales de proveedores de cloud, etc.

5 de febrero de 2023

Conector 3.9.26

- En la página **Iniciar sesión**, ahora se le pedirá que introduzca la dirección de correo electrónico asociada a su inicio de sesión. Después de hacer clic en **Siguiente**, BlueXP le solicita que realice la autenticación mediante el método de autenticación asociado a su inicio de sesión:
 - La contraseña de sus credenciales de cloud de NetApp
 - Sus credenciales de identidad federadas
 - Sus credenciales del sitio de soporte de NetApp

- Si es nuevo en BlueXP y tiene credenciales actuales del sitio de soporte de NetApp (NSS), puede omitir la página de registro e introducir su dirección de correo electrónico directamente en la página de inicio de sesión. BlueXP te inscribirá como parte de este inicio de sesión inicial.
- Al suscribirse a BlueXP desde el mercado de su proveedor de la nube, ahora tiene la opción de reemplazar la suscripción existente para una cuenta por la nueva suscripción.

Subscription Assignment

✓ Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name

QAAccount_Sub2Test-PAYGOByTheHourByCapacity

Select the NetApp accounts that you'd like to associate this subscription with. You can automatically replace the existing subscription for one account with this new subscription.

Netapp account	Replace existing subscription
<input checked="" type="checkbox"/> MyAccount	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/> Netapp-Kobi	<input type="checkbox"/>
<input checked="" type="checkbox"/> KeystoneTest01	<input type="checkbox"/>
<input checked="" type="checkbox"/> MyAccount	<input type="checkbox"/>

Save

- ["Aprenda a asociar una suscripción a AWS"](#)
- ["Aprenda a asociar una suscripción a Azure"](#)
- ["Descubra cómo asociar una suscripción a Google Cloud"](#)
- BlueXP le notificará ahora si su conector ha sido apagado durante 14 días o más.
 - ["Más información sobre las notificaciones de BlueXP"](#)
 - ["Descubra por qué los conectores deben seguir funcionando"](#)
- Hemos actualizado la política de Connector para Google Cloud para incluir el permiso necesario para crear y gestionar máquinas virtuales de almacenamiento en pares de alta disponibilidad de Cloud Volumes ONTAP:

compute.instances.updateNetworkInterface

["Vea los permisos de Google Cloud para Connector"](#).

- Esta versión del conector incluye mejoras de Cloud Volumes ONTAP.

["Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"](#)

1 de enero de 2023

Conector 3.9.25

Esta versión del conector incluye mejoras y correcciones de errores de Cloud Volumes ONTAP.

["Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"](#)

4 de diciembre de 2022

Conector 3.9.24

- Hemos actualizado la URL de la consola BlueXP a: <https://console.bluexp.netapp.com>
- El conector ahora es compatible con la región de Google Cloud Israel.
- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP y mejoras del clúster de ONTAP en las instalaciones.
 - ["Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"](#)
 - ["Obtenga información acerca de las mejoras del clúster en las instalaciones de ONTAP"](#)

6 de noviembre de 2022

Conector 3.9.23

- Sus suscripciones a PAYGO y los contratos anuales para BlueXP ya están disponibles para su visualización y gestión desde Digital Wallet.

["Obtenga información sobre cómo administrar sus suscripciones"](#)

- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP.

["Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"](#)

1 de noviembre de 2022

Cloud Manager ahora le solicita que actualice las credenciales asociadas con sus cuentas del sitio de soporte de NetApp cuando el token de actualización asociado con su cuenta caduque después de 3 meses. ["Aprenda a gestionar cuentas de NSS"](#)

18 de septiembre de 2022

Conector 3.9.22

- Hemos mejorado el asistente de despliegue de conectores añadiendo una *guía in-product* que proporciona los pasos necesarios para cumplir los requisitos mínimos de instalación del conector: Permisos, autenticación y redes.
- Ahora puede crear un caso de soporte de NetApp directamente desde Cloud Manager en **Support**

Dashboard.

["Aprenda a crear un caso"](#).

- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP.

["Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"](#)

31 de julio de 2022

Conector 3.9.21

- Hemos introducido una nueva forma de descubrir los recursos de cloud que ya no se están gestionando en Cloud Manager.

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

En esta versión inicial, My Opportunities le permite descubrir los sistemas de archivos FSX para ONTAP existentes en su cuenta de AWS.

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

- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP.

["Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"](#)

15 de julio de 2022

Cambios en las políticas

Hemos actualizado la documentación añadiendo las políticas de Cloud Manager directamente dentro de los documentos. Esto significa que ahora puede ver los permisos necesarios para el conector y Cloud Volumes ONTAP junto con los pasos que describen cómo configurarlos. Antes, estas políticas eran accesibles desde una página del sitio de soporte de NetApp.

["A continuación se muestra un ejemplo en el que se muestran los permisos de la función IAM de AWS que se utilizan para crear un conector"](#).

También hemos creado una página que proporciona enlaces a cada una de las políticas. ["Consulte el resumen de permisos de Cloud Manager"](#).

3 de julio de 2022

Conector 3.9.20

- Hemos introducido una nueva forma de acceder a la lista creciente de funciones en la interfaz de Cloud Manager. Ahora es posible disfrutar de todas las conocidas funcionalidades de Cloud Manager si pasa por el panel izquierdo.



- Ahora puede configurar Cloud Manager para que envíe notificaciones por correo electrónico, de modo que se le pueda informar de la actividad importante del sistema incluso si no ha iniciado sesión en el sistema.

["Obtenga más información sobre cómo supervisar operaciones en su cuenta"](#).

- Cloud Manager ahora admite almacenamiento Azure Blob y Google Cloud Storage como entornos de trabajo, similar a la compatibilidad de Amazon S3.

Después de instalar un conector en Azure o Google Cloud, Cloud Manager ahora detecta automáticamente información sobre el almacenamiento de Azure Blob en su suscripción a Azure o Google Cloud Storage en el proyecto donde está instalado el conector. Cloud Manager muestra el almacenamiento de objetos como entorno de trabajo que se puede abrir para ver información más detallada.

A continuación mostramos un ejemplo de un entorno de trabajo de Azure Blob:

1001

Azure blob

Overview

1001

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

- Hemos rediseñado la página de recursos para un entorno de trabajo de Amazon S3. Para ello, proporciona información más detallada sobre bloques S3, como la capacidad, detalles de cifrado, etc.
- Ahora el conector es compatible con las siguientes regiones de Google Cloud:
 - Madrid (europa-sur-oeste)
 - París (europa-West9)
 - Varsovia (Europa central 2)
- El conector ahora es compatible con Azure West US 3.

["Consulte la lista completa de las regiones admitidas"](#)

- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP.

["Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"](#)

28 de junio de 2022

Inicie sesión con las credenciales de NetApp

Cuando los nuevos usuarios se registren en Cloud Central, ahora podrán seleccionar la opción **Iniciar sesión con NetApp** para iniciar sesión con sus credenciales del sitio de soporte de NetApp. Esta es una alternativa para introducir una dirección de correo electrónico y una contraseña.



Los inicios de sesión existentes que utilizan una dirección de correo electrónico y una contraseña deben seguir utilizando ese método de inicio de sesión. La opción Iniciar sesión con NetApp está disponible para los nuevos usuarios que se registren.

7 de junio de 2022

Conector 3.9.19

- El conector ahora es compatible con la región de AWS Jakarta (AP-sureste-3).

- El conector ahora es compatible con la región sureste de Azure Brazil.

["Consulte la lista completa de las regiones admitidas"](#)

- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP y mejoras del clúster de ONTAP en las instalaciones.
 - ["Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"](#)
 - ["Obtenga información acerca de las mejoras del clúster en las instalaciones de ONTAP"](#)

12 de mayo de 2022

Parche del conector 3.9.18

Hemos actualizado el conector para introducir correcciones de errores. La solución más destacable es un problema que afecta a la puesta en marcha de Cloud Volumes ONTAP en Google Cloud cuando el conector se encuentra en un VPC compartido.

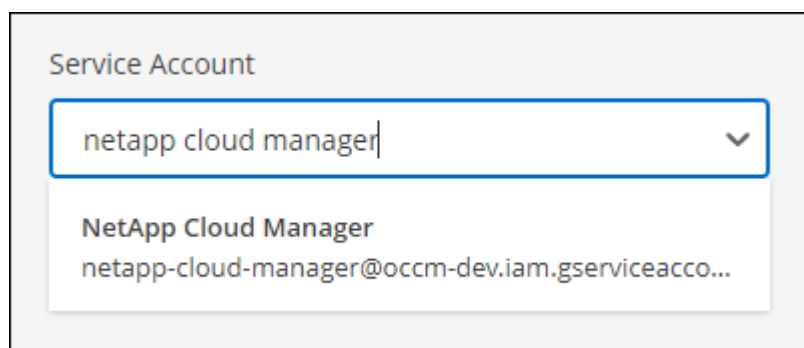
2 de mayo de 2022

Conector 3.9.18

- Ahora el conector es compatible con las siguientes regiones de Google Cloud:
 - Delhi (asia-sur-2)
 - Melbourne (australia-southeast2)
 - Milán (europa-west8)
 - Santiago (sur-oeste)

["Consulte la lista completa de las regiones admitidas"](#)

- Al seleccionar la cuenta de servicio de Google Cloud que se va a utilizar con Connector, Cloud Manager ahora muestra la dirección de correo electrónico asociada con cada cuenta de servicio. La visualización de la dirección de correo electrónico puede facilitar la distinción entre cuentas de servicio que comparten el mismo nombre.



- Hemos certificado Connector en Google Cloud en una instancia de máquina virtual con un sistema operativo compatible ["Características de VM blindadas"](#)
- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP. ["Obtenga información sobre estas mejoras"](#)
- Se necesitan nuevos permisos de AWS para que el conector ponga en marcha Cloud Volumes ONTAP.

Ahora es necesario obtener los siguientes permisos para crear un grupo de colocación extendido de AWS al implementar un par de alta disponibilidad en una única zona de disponibilidad (AZ):

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy"
```

Ahora se requieren estos permisos para optimizar la forma en que Cloud Manager crea el grupo de colocación.

Asegúrese de proporcionar estos permisos a cada conjunto de credenciales de AWS que haya añadido a Cloud Manager. ["Consulte la política de IAM más reciente para el conector"](#).

3 de abril de 2022

Conector 3.9.17

- Ahora puede crear un conector si deja que Cloud Manager asuma la función IAM que configuró en el entorno. Este método de autenticación es más seguro que compartir una clave de acceso y una clave secreta de AWS.

["Aprenda a crear un conector con el rol IAM"](#).

- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP. ["Obtenga información sobre estas mejoras"](#)

27 de febrero de 2022

Conector 3.9.16

- Al crear un nuevo conector en Google Cloud, Cloud Manager ahora mostrará todas sus políticas de firewall existentes. Anteriormente, Cloud Manager no mostraba ninguna política que no tuviera una etiqueta de destino.
- Esta versión del conector también incluye mejoras de Cloud Volumes ONTAP. ["Obtenga información sobre estas mejoras"](#)

30 de enero de 2022

Conector 3.9.15

Esta versión del conector incluye mejoras de Cloud Volumes ONTAP. ["Obtenga información sobre estas mejoras"](#)

2 de enero de 2022

Puntos finales reducidos para el conector

Hemos reducido el número de extremos con los que debe ponerse en contacto un conector para gestionar recursos y procesos en su entorno de cloud público.

["Consulte la lista de los extremos necesarios"](#)

Cifrado de disco EBS para el conector

Al implementar un nuevo conector en AWS desde Cloud Manager, ahora puede elegir cifrar los discos EBS del conector con la clave maestra predeterminada o una clave administrada.

The screenshot displays the 'Details' configuration page for an AWS connector instance. At the top, a progress bar shows six steps: 'Get Ready', 'AWS Credentials', 'Details' (current), 'Network', 'Security Group', and 'Review'. The 'Details' section includes a 'Connector Instance Name' field with the value 'Connector1'. To the right, the 'Connector Role' is set to 'Create Role'. Below this, the 'Role Name' is 'Cloud-Manager-Operator-9yils3K'. A black arrow points to the 'AWS Managed Encryption' toggle switch, which is currently turned on. Below the toggle, the 'Master Key' is 'aws/ebs (default)' with a 'Change Key' link. On the left side, there is a link to 'Add Tags to Connector Instance'.

Dirección de correo electrónico de las cuentas de NSS

Cloud Manager ahora puede mostrar la dirección de correo electrónico asociada con una cuenta del sitio de soporte de NetApp.



28 de noviembre de 2021

Actualización necesaria para las cuentas del sitio de soporte de NetApp

A partir de diciembre 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, Cloud Manager le solicitará que actualice las credenciales de las cuentas del sitio de soporte de NetApp existentes que haya añadido anteriormente.

Si todavía no ha migrado su cuenta de NSS a IDaaS, primero debe migrar la cuenta y, a continuación, actualizar sus credenciales en Cloud Manager.

- ["Aprenda a actualizar una cuenta de NSS con el nuevo método de autenticación".](#)
- ["Obtenga más información sobre el uso de Microsoft Azure AD por parte de NetApp para la gestión de identidades"](#)

Cambiar las cuentas de NSS para Cloud Volumes ONTAP

Si su organización tiene varias cuentas en la página de soporte de NetApp, ahora puede cambiar qué cuenta está asociada a un sistema Cloud Volumes ONTAP.

["Aprenda a conectar un entorno de trabajo a una cuenta de NSS diferente".](#)

4 de noviembre de 2021

Certificación SOC 2 de tipo 2

Una empresa independiente certificada de contables y un auditor de servicios examinaron Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense y Cloud Backup (plataforma Cloud Manager), y afirmaron que han obtenido los informes de SOC 2 de tipo 2 basados en los criterios aplicables de los servicios de confianza.

["Consulte los informes de SOC 2 de NetApp".](#)

El conector ya no es compatible como proxy

Ya no puede utilizar el conector de Cloud Manager como servidor proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP. Esta funcionalidad se ha eliminado y ya no se admite. Necesitará proporcionar conectividad AutoSupport a través de una instancia NAT o de los servicios proxy del entorno.

["Obtenga más información sobre la verificación de AutoSupport con Cloud Volumes ONTAP"](#)

31 de octubre de 2021

Autenticación con principal de servicio

Al crear un conector nuevo en Microsoft Azure, ahora puede autenticarse con un director de servicio de Azure, en lugar de con las credenciales de cuenta de Azure.

["Aprenda a autenticarse con un director de servicio de Azure".](#)

Mejora de credenciales

Hemos rediseñado la página de credenciales para facilitar su uso y lograr que coincida con el aspecto actual de la interfaz de Cloud Manager.

2 de septiembre de 2021

Se ha agregado un nuevo servicio de notificación

El servicio de notificación se ha introducido de modo que puede ver el estado de las operaciones de Cloud Manager que ha iniciado durante su sesión actual. Puede verificar si la operación se ha realizado correctamente o si ha fallado. ["Consulte cómo se supervisan las operaciones de la cuenta".](#)

1 de agosto de 2021

Compatibilidad con RHEL 7.9 con el conector

El conector ahora es compatible con un host que ejecuta Red Hat Enterprise Linux 7.9.

["Ver los requisitos del sistema para el conector".](#)

7 de julio de 2021

Mejoras en el asistente Agregar conector

Hemos rediseñado el asistente **Add Connector** para añadir nuevas opciones y facilitar su uso. Ahora puede

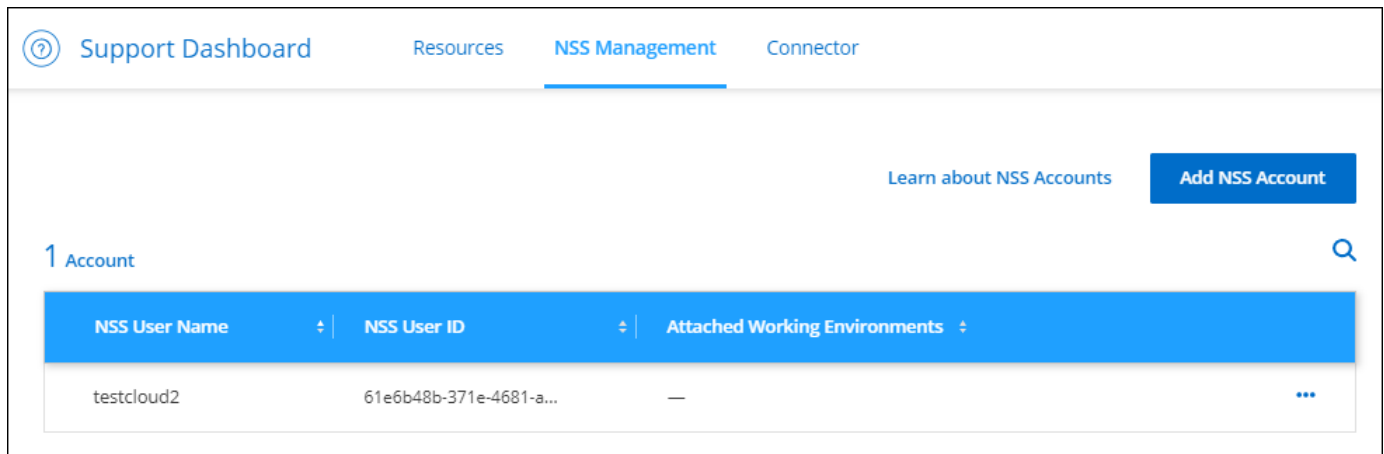
añadir etiquetas, especificar un rol (para AWS o Azure), cargar un certificado raíz para un servidor proxy, ver código para la automatización de Terraform, ver detalles del progreso, etc.

- ["Cree un conector en AWS"](#)
- ["Cree un conector en Azure"](#)
- ["Cree un conector en GCP"](#)

Gestión de cuentas de NSS desde la consola de soporte

Las cuentas del sitio de soporte de NetApp (NSS) ahora se gestionan desde la consola de soporte, en lugar de hacerlo desde el menú Configuración. Este cambio facilita la búsqueda y la gestión de toda la información relacionada con el soporte desde una única ubicación.

["Aprenda a gestionar cuentas de NSS"](#).



5 de mayo de 2021

Cuentas en la línea de tiempo

La línea de tiempo de Cloud Manager ahora muestra acciones y eventos relacionados con la gestión de cuentas. Las acciones incluyen cosas como asociar usuarios, crear áreas de trabajo y crear conectores. 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.

["Aprenda a filtrar la línea de tiempo al servicio de tenancy"](#).

11 de abril de 2021

API llama directamente a Cloud Manager

Si configuró un servidor proxy, ahora puede habilitar una opción para enviar llamadas API directamente a Cloud Manager sin pasar por el proxy. Esta opción es compatible con conectores que se ejecutan en AWS o en Google Cloud.

["Obtenga más información sobre este ajuste"](#).

Usuarios de cuentas de servicio

Ahora puede crear un usuario de cuenta de servicio.

Una cuenta de servicio actúa como un "usuario" que puede realizar llamadas API autorizadas a Cloud Manager 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.

["Obtenga más información acerca del uso de cuentas de servicio".](#)

Vistas previas privadas

Ahora puede permitir que las vistas previas privadas de su cuenta obtengan acceso a nuevos servicios cloud de NetApp conforme vayan disponibles como vista previa en Cloud Manager.

["Obtenga más información sobre esta opción".](#)

Servicios de terceros

También puede permitir que los servicios de terceros de su cuenta tengan acceso a servicios de terceros disponibles en Cloud Manager.

["Obtenga más información sobre esta opción".](#)

9 de febrero de 2021

Mejoras en la consola de soporte

Hemos actualizado la consola de soporte de con el fin de permitirle añadir sus credenciales del sitio de soporte de NetApp, que le registra para recibir soporte. También puede iniciar un caso de soporte de NetApp directamente desde la consola. Simplemente haga clic en el icono Ayuda y luego **Soporte**.

Limitaciones conocidas

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o cuya interoperabilidad con esta no es óptima. Revise estas limitaciones detenidamente.

Estas limitaciones son específicas para la configuración y administración de BlueXP: El conector, la plataforma SaaS, y más.

Limitaciones del conector

Posible conflicto con las direcciones IP en el rango 172

BlueXP despliega el conector con dos interfaces que tienen direcciones IP en las gamas 172.17.0.0/16 y 172.18.0.0/16.

Si la red tiene una subred configurada con cualquiera de estos rangos, puede que experimente errores de conectividad de BlueXP. Por ejemplo, la detección de clústeres de ONTAP en las instalaciones en BlueXP podría fallar.

Consulte el artículo de Knowledge base ["BlueXP Connector IP entra en conflicto con la red existente"](#) Para obtener instrucciones sobre cómo cambiar la dirección IP de las interfaces del conector.

El descifrado SSL no es compatible

BlueXP no admite configuraciones de firewall que tengan activado el descifrado SSL. Si está activado el descifrado SSL, aparecerán mensajes de error en BlueXP y la instancia del conector aparecerá como inactiva.

Para mejorar la seguridad, tiene la opción de ["Instalar un certificado HTTPS firmado por una entidad de certificación \(CA\)"](#).

Página en blanco al cargar la interfaz de usuario local

Si carga la interfaz de usuario local para un conector, es posible que la interfaz de usuario no se muestre a veces y solo se obtiene una página en blanco.

Este problema está relacionado con un problema del almacenamiento en caché. La solución alternativa es usar una sesión de navegador web privada o de incógnito.

No se admiten los hosts Linux compartidos

El conector no es compatible con una máquina virtual compartida con otras aplicaciones. La máquina virtual debe estar dedicada al software del conector.

agentes y extensiones de terceros

No se admiten agentes de terceros ni extensiones de VM en el conector VM.

Limitaciones de SaaS

La plataforma SaaS está deshabilitada para las regiones gubernamentales

Si implementa un conector en una región de AWS GovCloud, una región de Azure Gov o una región de Azure DoD, el acceso a BlueXP solo está disponible a través de la dirección IP de host de un conector. El acceso a la plataforma SaaS está desactivado para toda la cuenta.

Esto significa que solo los usuarios con privilegios que pueden acceder al VPC/vnet interno del usuario final pueden usar la interfaz de usuario o la API de BlueXP.

Tenga en cuenta que los únicos servicios que se admiten en estas regiones son Cloud Volumes ONTAP, Cloud Backup, Cloud Data Sense y Replication. No se ofrece soporte a otros servicios de NetApp en regiones gubernamentales.

["Aprenda a acceder a la interfaz de usuario local en el conector"](#).

Manos a la obra

Más información sobre BlueXP

BlueXP (anteriormente Cloud Manager) permite que los expertos en TECNOLOGÍA y los arquitectos de cloud gestionen de forma centralizada su infraestructura multicloud híbrida con las soluciones cloud de NetApp.

Funciones

BlueXP es una plataforma de gestión basada en SaaS de nivel empresarial que le permite controlar sus datos sin importar dónde se encuentren.

- Configuración y uso ["Cloud Volumes ONTAP"](#) para lograr una gestión de datos eficiente con varios protocolos en todos los clouds.
- Configure y utilice los servicios cloud de almacenamiento de archivos:
 - ["Azure NetApp Files"](#)
 - ["Amazon FSX para ONTAP"](#)
 - ["Cloud Volumes Service para Google Cloud"](#)
- Detectar y gestionar ["almacenamiento en las instalaciones"](#)
 - Sistemas E-Series
 - Clústeres ONTAP
 - Sistemas StorageGRID
- Utilice los servicios de BlueXP para la movilidad, la protección y el análisis y el control de los datos:
 - ["Backup en el cloud"](#)
 - ["Cloud Data SENSE"](#)
 - ["Cloud Sync"](#)
 - ["Organización en niveles del cloud"](#)
 - ["Asesor digital"](#)
 - ["Caché de archivos global"](#)
 - ["Kubernetes"](#)
 - ["Protección contra ransomware"](#)
 - ["Replicación"](#)

["Más información sobre BlueXP"](#)

Proveedores de cloud compatibles

BlueXP le permite gestionar el almacenamiento en cloud y utilizar servicios cloud en Amazon Web Services, Microsoft Azure y Google Cloud.

Coste

El precio de BlueXP depende de los servicios que usted planea utilizar. ["Más información sobre los precios de BlueXP"](#).

Cómo funciona BlueXP

BlueXP incluye una interfaz basada en SaaS que está integrada con el sitio web de BlueXP y conectores que gestionan Cloud Volumes ONTAP y otros servicios en la nube.

Software como servicio

BlueXP es accesible a través de un ["Interfaz de usuario basada en SaaS"](#) Y API. Esta experiencia de SaaS le permite acceder automáticamente a las últimas funciones de su lanzamiento y cambiar fácilmente entre sus cuentas y conectores de NetApp.



Si trabaja en un entorno en el que no hay acceso saliente a Internet, puede instalar el software Connector en ese entorno y acceder a la interfaz de usuario local que está disponible en el conector. ["Más información sobre conectores"](#).

Página web de BlueXP

["El sitio web de BlueXP"](#) proporciona una ubicación centralizada para acceder y gestionar ["Servicios en nube de NetApp"](#). Con la autenticación de usuario centralizada, puede utilizar el mismo conjunto de credenciales para acceder a BlueXP y otros servicios en la nube como Cloud Insights.

Cuenta de NetApp

Cuando inicie sesión en BlueXP por primera vez, se le solicitará que cree una cuenta *NetApp*. Esta cuenta proporciona multi-tenancy y le permite organizar usuarios y recursos en espacios de trabajo aislados.

Conectores

En la mayoría de los casos, un administrador de cuentas de BlueXP necesitará poner en marcha un *Connector* en su red local o en la nube. Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público.

["Obtenga más información sobre cuándo se necesitan los conectores y cómo trabajo"](#).

Certificación SOC 2 de tipo 2

Una empresa independiente certificada de contables y un auditor de servicios examinaron BlueXP, Cloud Sync, Cloud Tiering, Cloud Data Sense y Cloud Backup (plataforma BlueXP) y afirmaron que han obtenido los informes de SOC 2 tipo 2 basados en los criterios aplicables de los servicios de confianza.

["Consulte los informes de SOC 2 de NetApp"](#)

Lista de comprobación de introducción

Utilice esta lista de comprobación para comprender lo que se necesita para empezar a trabajar con BlueXP en una implementación típica en la que el conector tenga acceso saliente a Internet.

Un inicio de sesión

Para iniciar sesión en BlueXP, puede utilizar sus credenciales del sitio de soporte de NetApp o puede registrarse para iniciar sesión en cloud de NetApp con su correo electrónico y una contraseña. ["Obtenga más información sobre cómo iniciar sesión"](#).

Acceso a la red desde un explorador Web hasta varios puntos finales

Se puede acceder a la interfaz de usuario de BlueXP desde un navegador Web. Al utilizar la interfaz de usuario de BlueXP, se pone en contacto con varios extremos para completar las tareas de gestión de datos. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales.


Puntos finales	Específico
https://console.bluexp.netapp.com	Su explorador web se pone en contacto con esta URL cuando utiliza la interfaz de usuario de SaaS.
Servicios de AWS (amazonaws.com): <ul style="list-style-type: none">• Formación CloudFormation• Cognito• Cloud computing elástico (EC2)• Servicio de gestión de claves (KMS)• Servicio de token de seguridad (STS)• Simple Storage Service (S3)	Necesario para implementar un conector desde BlueXP en AWS. El extremo exacto depende de la región en la que se despliega el conector. "Consulte la documentación de AWS para obtener más detalles."
https://management.azure.com https://login.microsoftonline.com	Necesario para implementar un conector desde BlueXP en la mayoría de las regiones de Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Necesario para implementar un conector desde BlueXP en las regiones de Alemania de Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Necesario para desplegar un conector desde BlueXP en las regiones de la Gov de los EE. UU. De Azure.
https://www.googleapis.com	Necesario para desplegar un conector de BlueXP en Google Cloud.
https://signin.b2c.netapp.com	Se requiere actualizar las credenciales del sitio de soporte de NetApp (NSS) o añadir nuevas credenciales de NSS a BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	El explorador Web se conecta a estos extremos para una autenticación de usuario centralizada a través de BlueXP.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Red de salida para un conector

Después de iniciar sesión en BlueXP, un administrador de cuentas de BlueXP necesitará implementar un *Connector* en un proveedor de nube o en su red local. Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público. Tenga en cuenta que se necesita un conector para la mayoría, pero no todos los servicios y funciones de BlueXP. ["Obtenga más información sobre conectores y cómo funcionan"](#).

- La ubicación de red en la que implemente el conector debe tener una conexión a Internet saliente.

El conector requiere acceso saliente a Internet para ponerse en contacto con los siguientes extremos con el fin de gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
https://<region>.amazonaws.com	Para gestionar recursos en AWS.
https://management.azure.com https://login.microsoftonline.com	Para gestionar recursos en regiones públicas de Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us	Para gestionar recursos en regiones gubernamentales de Azure.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud	Para administrar recursos en la región de Azure IL6.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://www.googleapis.com/compute/v1/ https://cloudresourcemanager.googleapis.com/v1/ projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/ v2/projects	Para gestionar recursos en Google Cloud.
https://support.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.bluelxp.netapp.com https://api.bluelxp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	<div>  <p>El conector se está comunicando actualmente con "cloudmanager.cloud.netapp.com" pero empezará a ponerse en contacto con "api.bluelxp.netapp.com" en una próxima versión.</p> </div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Para actualizar el conector y sus componentes de Docker.

- Si decide instalar manualmente el conector en su propio host Linux (y no hacerlo directamente desde la interfaz de BlueXP), el instalador del conector requiere acceso a varios puntos finales durante el proceso de instalación:

["Revise la lista de extremos".](#)

- No hay tráfico entrante en el conector, a menos que lo inicie.

HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras

circunstancias. SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas. Mientras tanto, se requieren conexiones de entrada a través del puerto 3128 si implementa sistemas Cloud Volumes ONTAP en una subred donde no hay una conexión de Internet de salida disponible.

Permisos del proveedor de cloud

Necesita una cuenta que tenga permisos para implementar el conector en su proveedor de nube directamente desde BlueXP.



Existen formas alternativas de crear un conector: Puede crear un conector a partir de "[Mercado AWS](#)", la "[Azure Marketplace](#)", o usted puede "[instale manualmente el software](#)".

Ubicación	Escalones de alto nivel	Pasos detallados
AWS	<ol style="list-style-type: none">1. Utilice un archivo JSON que incluya los permisos necesarios para crear una política de IAM en AWS.2. Asocie la política a un usuario de IAM o IAM.3. Al crear el conector, proporcione a BlueXP el ARN de la función IAM o la clave de acceso y la clave secreta de AWS para el usuario de IAM.	"Haga clic aquí para ver los pasos detallados" .
Azure	<ol style="list-style-type: none">1. Utilice un archivo JSON que incluya los permisos necesarios para crear un rol personalizado en Azure.2. Asigne la función al usuario que creará el conector desde BlueXP.3. Al crear el conector, inicie sesión con la cuenta de Microsoft que tiene los permisos necesarios (el indicador de inicio de sesión que es propiedad de Microsoft y está alojado en él).	"Haga clic aquí para ver los pasos detallados" .
Google Cloud	<ol style="list-style-type: none">1. Utilice un archivo YAML que incluya los permisos necesarios para crear una función personalizada en Google Cloud.2. Adjunte esa función al usuario que creará el conector desde BlueXP.3. Si piensa utilizar Cloud Volumes ONTAP, configure una cuenta de servicio que tenga los permisos necesarios.4. Habilite las API de Google Cloud.5. Al crear el conector, inicie sesión con la cuenta de Google que tiene los permisos necesarios (Google es propietario y está alojado en la solicitud de inicio de sesión).	"Haga clic aquí para ver los pasos detallados" .

Creación de redes para servicios individuales

Una vez completada la instalación, estará listo para empezar a utilizar los servicios disponibles en BlueXP. Tenga en cuenta que cada servicio tiene sus propios requisitos de red. Consulte las páginas siguientes para obtener más información.

- "Cloud Volumes ONTAP para AWS"
- "Cloud Volumes ONTAP para Azure"
- "Cloud Volumes ONTAP para GCP"
- "Replicación de datos entre sistemas ONTAP"
- "Poner en marcha Cloud Data Sense"
- "Clústeres de ONTAP en las instalaciones"
- "Organización en niveles del cloud"
- "Backup en el cloud"

Regístrese en BlueXP

Cuando comience con BlueXP, su primer paso es registrarse. Se le dará la opción de crear una cuenta, pero puede omitir ese paso si está siendo invitado a una cuenta existente.

Una nota sobre las regiones gubernamentales

Si necesita acceder a BlueXP desde una región gubernamental o un sitio que no tenga acceso saliente a Internet, debe crear un conector e iniciar sesión en la interfaz de usuario de BlueXP que se ejecuta localmente en el conector. ["Aprenda a acceder a la interfaz de usuario local en el conector"](#).

Opciones de registro

BlueXP es accesible desde su navegador web a través de una interfaz de usuario basada en SaaS.

Puede suscribirse a BlueXP mediante una de las siguientes opciones:

- Sus credenciales existentes del sitio de soporte de NetApp (NSS)
- Inicio de sesión en el cloud de NetApp especificando su dirección de correo electrónico y una contraseña

Ambas opciones admiten una conexión federada, que habilita el inicio de sesión único mediante credenciales del directorio corporativo (identidad federada). Después de registrarse, puede configurar una conexión federada desde ["Centro de ayuda de BlueXP"](#) seleccionando **Opciones de inicio de sesión de Cloud Central**.

Pasos

1. Abra un explorador web y vaya al ["Consola BlueXP"](#)
2. En la página **Iniciar sesión**, seleccione **Registrarse**.



Si tiene pensado utilizar sus credenciales de NSS existentes, puede omitir la página de registro e introducir su dirección de correo electrónico directamente en la página de inicio de sesión. BlueXP te inscribirá como parte de este inicio de sesión inicial.

3. En la página **Registrarse**, seleccione una de las opciones de inicio de sesión:
 - Si tiene una cuenta existente del sitio de soporte de NetApp (NSS), seleccione **Regístrese con sus credenciales del sitio de soporte de NetApp**.

Cuando usa esta opción, sus credenciales del sitio de soporte de NetApp (NSS) no se añaden a BlueXP en la consola de soporte. ["Aprenda a añadir sus credenciales de NSS a la consola de soporte para habilitar los flujos de trabajo clave"](#).

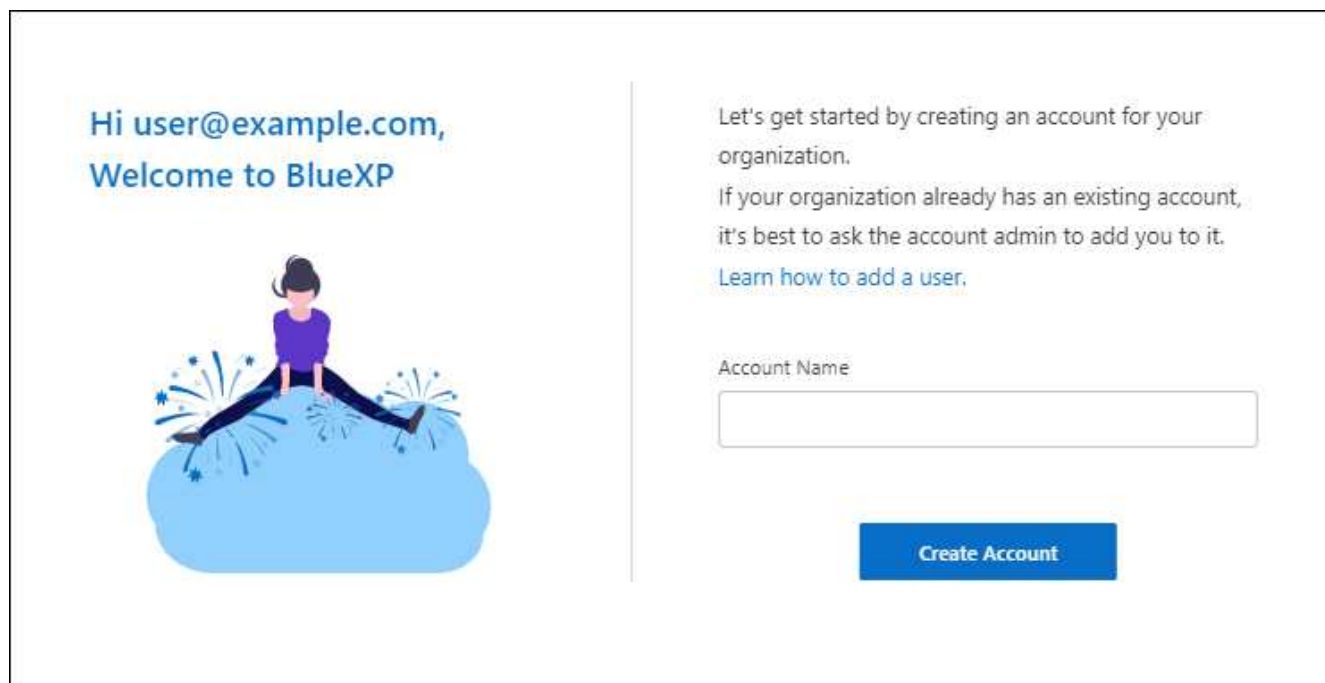
- Si no tiene una cuenta de NSS y no ha creado las credenciales de cloud de NetApp, introduzca la información requerida para crear un inicio de sesión en cloud de NetApp.

Tenga en cuenta que sólo se permiten caracteres ingleses en el formulario de registro.

4. Cuando se le solicite, revise el Contrato de licencia para el usuario final y acepte los términos.
5. En la página **bienvenida**, escriba un nombre para su cuenta.

Si su empresa ya tiene una cuenta y desea unirse a ella, debe omitir este paso y pedir al propietario que lo asocie a la cuenta. Una vez que el propietario le agregue, puede iniciar sesión y tendrá acceso a la cuenta. "[Aprenda a agregar miembros a una cuenta existente](#)".

Una cuenta es el elemento de nivel superior de la plataforma de identidades de NetApp. Permite añadir y gestionar usuarios, roles, permisos y entornos de trabajo.

The screenshot shows a welcome page for BlueXP. On the left, there is a blue cloud graphic with a person sitting on it, surrounded by starburst effects. Above the graphic, the text reads "Hi user@example.com, Welcome to BlueXP". On the right, there is a vertical line separating the welcome message from the account creation instructions. The instructions say: "Let's get started by creating an account for your organization. If your organization already has an existing account, it's best to ask the account admin to add you to it. [Learn how to add a user.](#)". Below this text is a text input field labeled "Account Name". At the bottom right, there is a blue button with the text "Create Account".

6. Seleccione **Crear cuenta**.

Resultado

Ahora tienes una cuenta y un inicio de sesión de BlueXP. En la mayoría de los casos, el siguiente paso es crear un conector que conecte los servicios de BlueXP a su entorno de nube híbrida.

Inicie sesión en BlueXP

Después de registrarse en BlueXP, puede iniciar sesión desde su navegador web a través de la interfaz de usuario basada en SaaS.

"[Aprenda cómo registrarse en BlueXP y crear una organización](#)".

Si accede a BlueXP desde una región gubernamental o un sitio que no tiene acceso saliente a Internet, deberá iniciar sesión en la interfaz de usuario de BlueXP que se ejecuta localmente en el conector. "[Aprenda a acceder a la interfaz de usuario local en el conector](#)".

Opciones de inicio de sesión

Puede iniciar sesión en BlueXP con una de las siguientes opciones:

- Sus credenciales existentes del sitio de soporte de NetApp (NSS)
- Un inicio de sesión en el cloud de NetApp con su dirección de correo electrónico y una contraseña
- Una conexión federada

Puede utilizar el inicio de sesión único para iniciar sesión con credenciales del directorio corporativo (identidad federada). Para obtener más información, visite la "[Centro de ayuda de BlueXP](#)" y, a continuación, haga clic en **opciones de inicio de sesión**.

Pasos

1. Abra un explorador web y vaya al "[Consola BlueXP](#)"
2. En la página **Iniciar sesión**, introduzca la dirección de correo electrónico asociada a su inicio de sesión.
3. En función del método de autenticación asociado a su inicio de sesión, se le pedirá que introduzca sus credenciales:
 - Credenciales de cloud de NetApp: Introduzca su contraseña
 - Federated user: Introduzca las credenciales de identidad federadas
 - Cuenta del sitio de soporte de NetApp: Introduzca sus credenciales del sitio de soporte de NetApp

Resultado

Ya ha iniciado sesión y puede empezar a utilizar BlueXP para gestionar su infraestructura multicloud híbrida.

Configure una cuenta de NetApp


Obtenga más información acerca de las cuentas de NetApp

A *NetApp account* proporciona multi-tenancy y le permite organizar usuarios y recursos en espacios de trabajo aislados desde BlueXP.

Por ejemplo, varios usuarios pueden implementar y administrar sistemas Cloud Volumes ONTAP en entornos aislados denominados *espacios de trabajo*. Estos espacios de trabajo son invisibles para otros usuarios, a menos que se compartan.

Cuando acceda por primera vez a BlueXP, se le solicitará que seleccione o cree una cuenta de NetApp:

Hi user@example.com,
Welcome to BlueXP



Let's get started by creating an account for your organization.
If your organization already has an existing account, it's best to ask the account admin to add you to it.
[Learn how to add a user.](#)


Account Name


Create Account


Los administradores de cuentas de BlueXP pueden modificar la configuración de esta cuenta gestionando usuarios (miembros), áreas de trabajo y conectores:


Manage Account: KeystoneTes...



OverviewMembersWorkspacesBlueXP Connector


30Members


1Workspaces

3Connectors

KeystoneTest01
Account Name

Allow Private Preview

account-Pq7bhQxz
Account ID

Allow Third Party Services

Para obtener instrucciones paso a paso, consulte ["Configuración de la cuenta de NetApp"](#).

Configuración de la cuenta

El widget Manage Account de BlueXP permite a los administradores de cuentas gestionar una cuenta de NetApp. Si acaba de crear su cuenta, entonces comenzará desde cero. Pero si ya ha configurado una cuenta, verá *All* los usuarios, espacios de trabajo y conectores asociados a la cuenta.

Descripción general

En la página Overview se muestran el Nombre de cuenta y el ID de cuenta. Es posible que tenga que proporcionar su ID de cuenta al registrar algunos servicios. Esta página también incluye algunas opciones de configuración de BlueXP.

Miembros

Los miembros son usuarios de BlueXP que usted asocia a su cuenta de NetApp. La asociación de un usuario con una cuenta y una o más áreas de trabajo de esa cuenta permite a esos usuarios crear y administrar entornos de trabajo en BlueXP.

Al asociar un usuario, debe asignarles un rol:

- *Account Admin*: Puede realizar cualquier acción en BlueXP.
- *Workspace Admin*: Puede crear y administrar recursos en el área de trabajo asignada.
- *Compliance Viewer*: Sólo puede ver la información de cumplimiento de Cloud Data Sense y generar informes para los sistemas a los que tienen permiso de acceso.
- *SnapCenter Admin*: Puede utilizar el servicio SnapCenter para crear copias de seguridad coherentes con las aplicaciones y restaurar datos utilizando dichas copias de seguridad. *Este servicio está actualmente en Beta.*

["Obtenga más información sobre estos roles"](#).

Espacios de trabajo

En BlueXP, un área de trabajo aísla cualquier número de *entornos de trabajo* de otros entornos de trabajo. Los administradores de área de trabajo no pueden acceder a los entornos de trabajo de un área de trabajo a menos que el administrador de cuentas asocie el administrador a ese espacio de trabajo.

Un entorno de trabajo representa un sistema de almacenamiento. Por ejemplo:

- Un sistema Cloud Volumes ONTAP
- Un clúster de ONTAP en las instalaciones
- Un clúster de Kubernetes

["Aprenda a agregar un área de trabajo"](#).

Conectores

A Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público. El conector se ejecuta en una instancia de máquina virtual que se implementa en su proveedor de cloud o en un host en las instalaciones que configuró.

Puede utilizar un conector con más de un servicio de datos en cloud de NetApp. Por ejemplo, si utiliza un conector para gestionar Cloud Volumes ONTAP, puede utilizar el mismo conector con otro servicio como Cloud Tiering.

["Más información sobre conectores"](#).

Ejemplos

Los siguientes ejemplos muestran cómo se pueden configurar las cuentas.

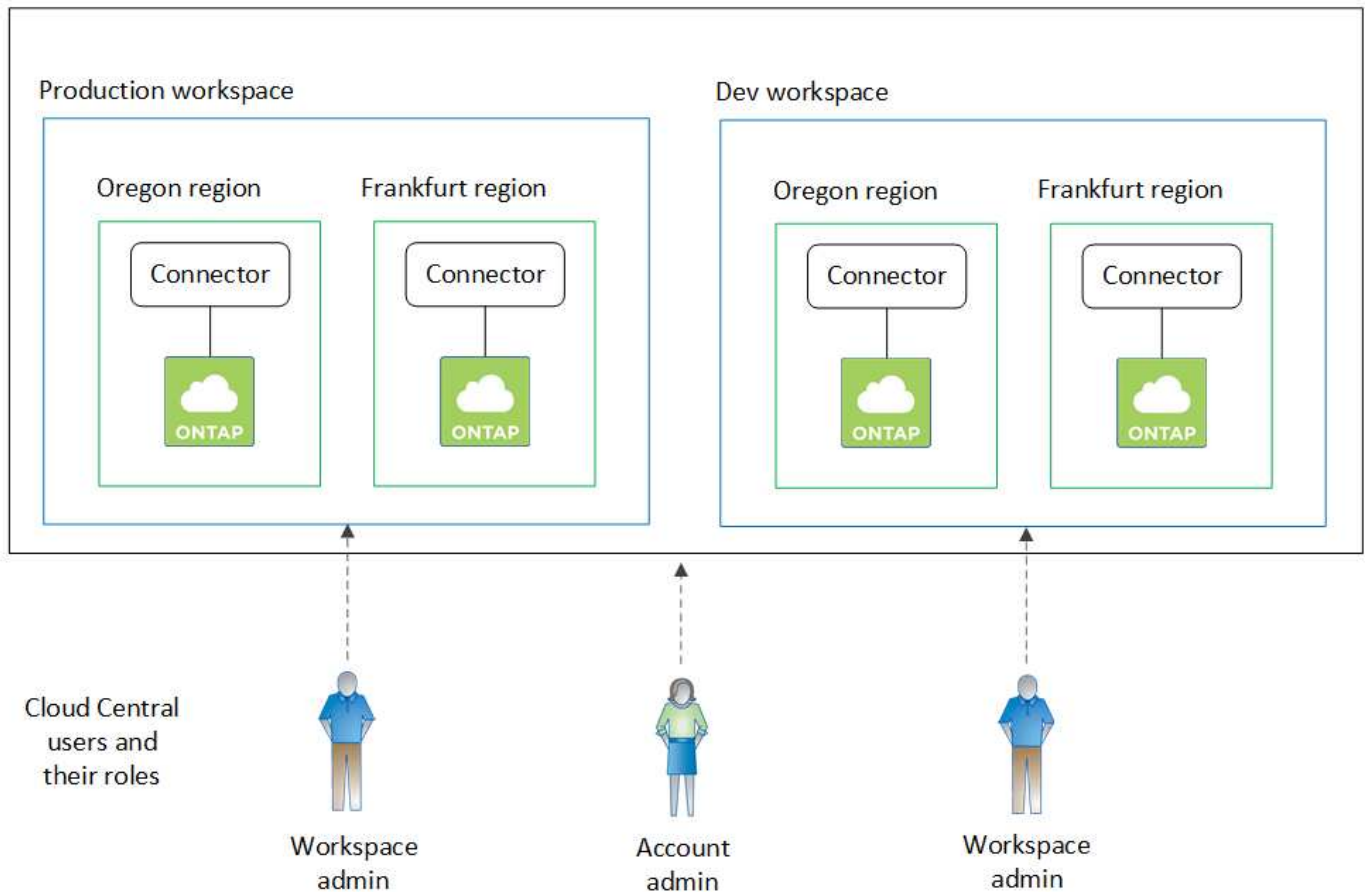


En las dos imágenes de ejemplo siguientes, el conector y los sistemas Cloud Volumes ONTAP no residen en la cuenta de NetApp, que se ejecutan en un proveedor de cloud. Ésta es una representación conceptual de la relación entre cada componente.

Ejemplo 1

En el ejemplo siguiente se muestra una cuenta que utiliza dos espacios de trabajo para crear entornos aislados. El primer espacio de trabajo es para un entorno de producción y el segundo para un entorno de desarrollo.

Account



Ejemplo 2

Aquí tenemos otro ejemplo que muestra el máximo nivel de multi-tenancy utilizando dos cuentas de NetApp independientes. Por ejemplo, un proveedor de servicios puede utilizar BlueXP en una cuenta para proporcionar servicios a sus clientes, mientras que usa otra cuenta para proporcionar recuperación ante desastres para una de sus unidades de negocio.

Tenga en cuenta que la cuenta 2 incluye dos conectores independientes. Esto puede suceder si tiene sistemas en regiones independientes o en proveedores de cloud independientes.



Configure espacios de trabajo y usuarios en su cuenta de NetApp

Cuando inicie sesión en BlueXP por primera vez, se le solicitará que cree una cuenta *NetApp*. Esta cuenta proporciona multi-tenancy y le permite organizar usuarios y recursos en espacios de trabajo aislados.

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

Configurar su cuenta de NetApp para que los usuarios puedan acceder a BlueXP y acceder a los entornos de trabajo de un espacio de trabajo. Solo tiene que añadir un único usuario o añadir varios usuarios y espacios de trabajo.

Agregar espacios de trabajo

En BlueXP, las áreas de trabajo permiten aislar un conjunto de entornos de trabajo de otros entornos de trabajo y de otros usuarios. Por ejemplo, puede crear dos espacios de trabajo y asociar usuarios independientes a cada espacio de trabajo.

Pasos

1. Desde lo alto de "BlueXP", Haga clic en el menú desplegable **cuenta**.



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



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

Después de terminar

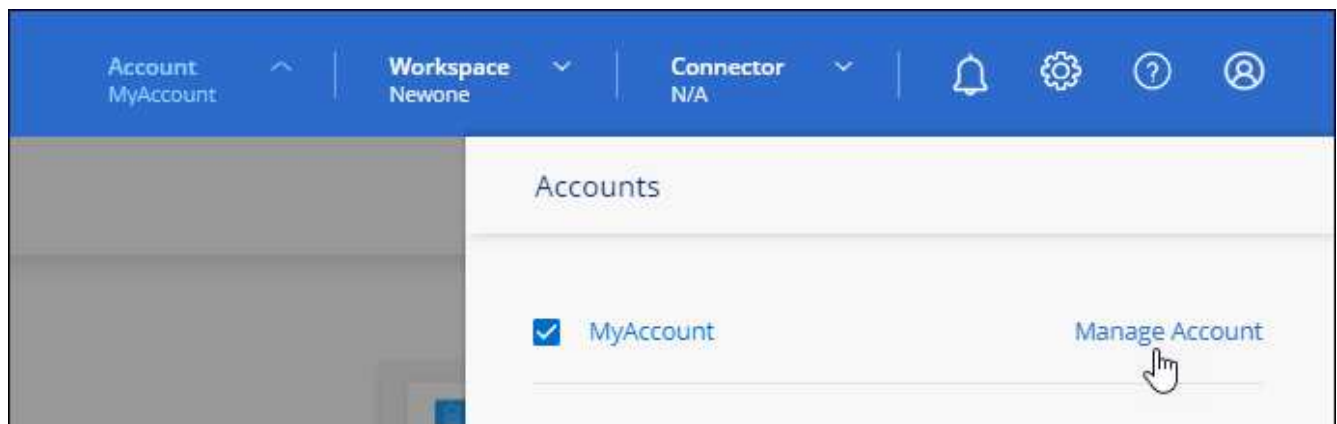
Si un administrador de área de trabajo necesita acceso a este área de trabajo, deberá asociarlo al usuario. También deberá asociar conectores al espacio de trabajo para que los administradores del área de trabajo puedan utilizar dichos conectores.

Añadir 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. Desde lo alto de ["BlueXP"](#), Haga clic en el menú desplegable **cuenta** y haga clic en **Administrar cuenta**.

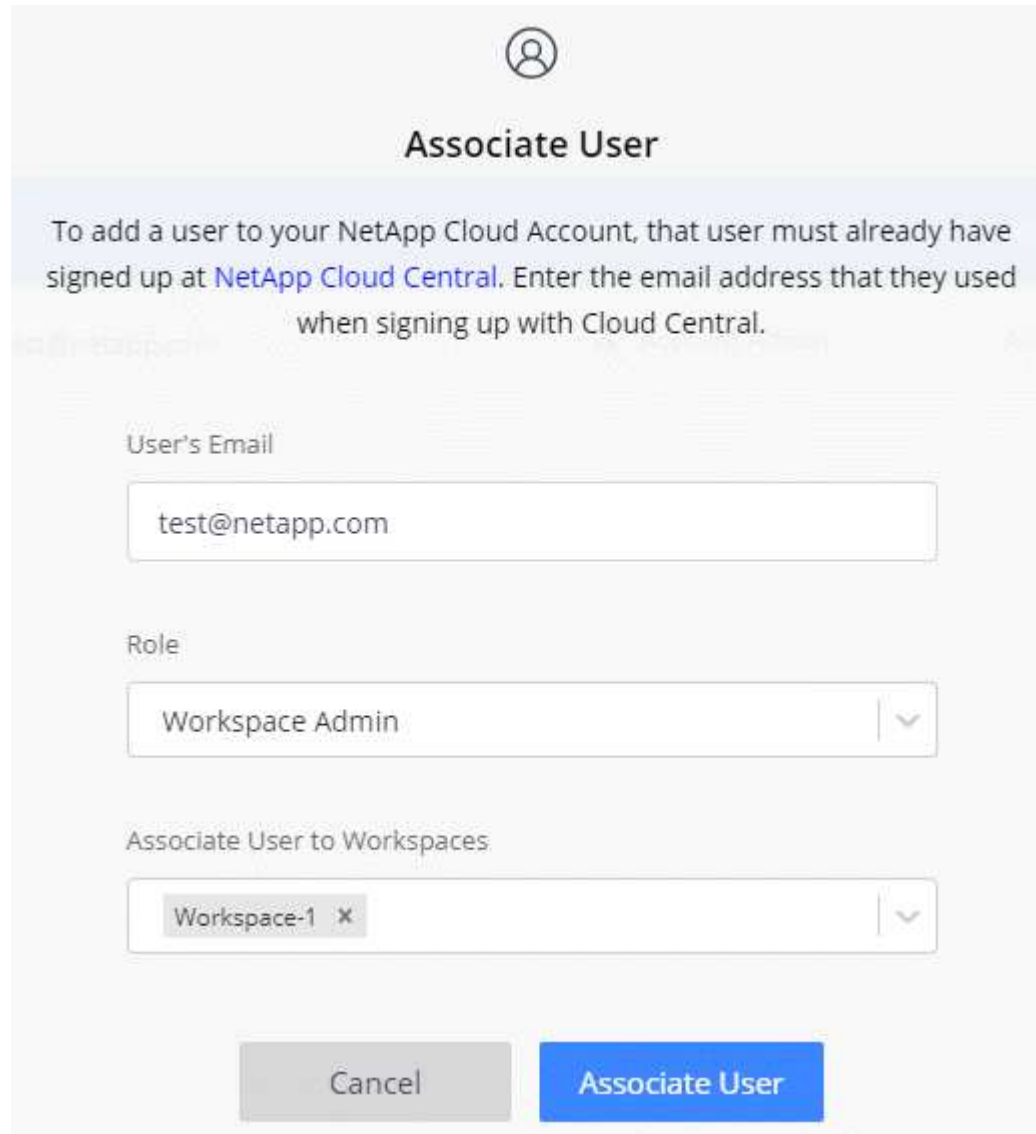


3. En la ficha Miembros, haga clic en **Usuario asociado**.
4. Introduzca la dirección de correo electrónico del usuario y seleccione un rol para el usuario:
 - **Administración de cuentas:** Puede realizar cualquier acción en BlueXP.
 - **Administración de área de trabajo:** Puede crear y administrar recursos en áreas de trabajo asignadas.
 - **Visor de cumplimiento:** Sólo puede ver información de cumplimiento y gobierno 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.

5. Si ha seleccionado una cuenta que no sea Administración de cuentas, seleccione uno o varios espacios de trabajo para asociarlos con ese usuario.



Associate User

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

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 X

Cancel Associate User

6. Haga clic en **asociar**.

Resultado

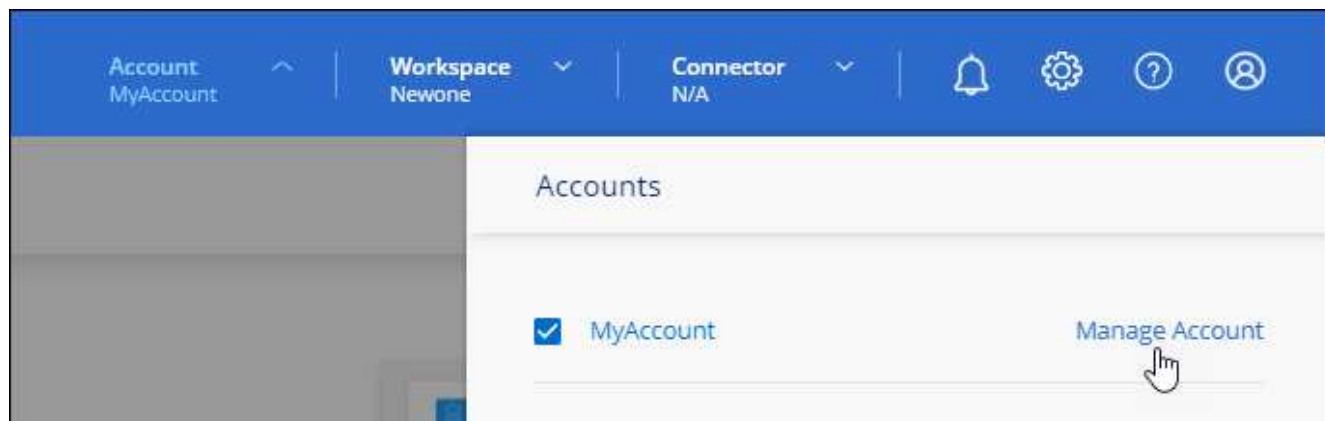
El usuario debe recibir un correo electrónico del sitio web de BlueXP de NetApp titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a BlueXP.

Asociar los administradores de área de trabajo a los espacios de trabajo

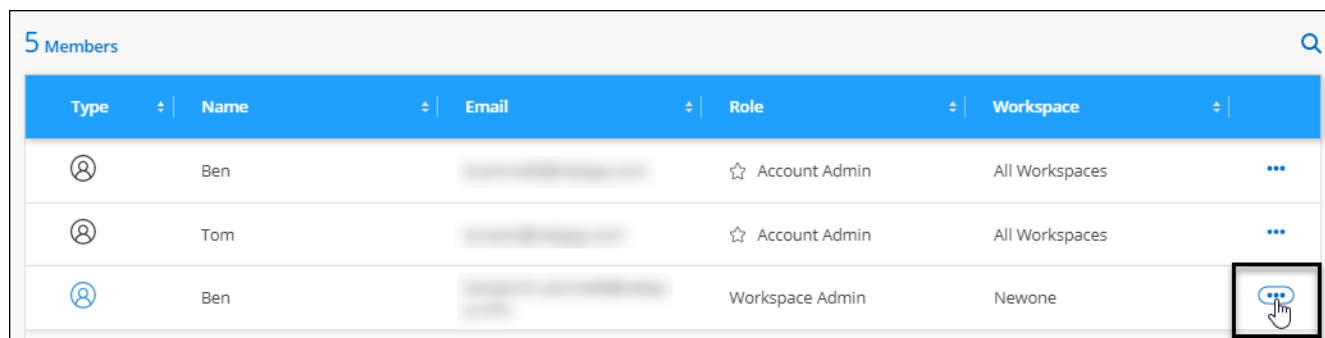
Puede asociar los administradores de área de trabajo a espacios de trabajo adicionales en cualquier momento. La asociación del usuario les permite crear y ver los entornos de trabajo en ese espacio de trabajo.

Pasos

1. 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 **Administrar espacios de trabajo**.
4. Seleccione uno o más espacios de trabajo 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.

Asociar conectores a áreas de trabajo

Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP.

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 uno o más espacios de trabajo y haga clic en **aplicar**.

Resultado

Los administradores de área de trabajo ahora pueden usar estos conectores para crear sistemas Cloud Volumes ONTAP.

El futuro

Ahora que ha configurado su cuenta, puede gestionarlo en cualquier momento eliminando usuarios, gestionando áreas de trabajo y gestionando conectores. ["Aprenda a administrar su cuenta"](#).

Configure un conector

Más información sobre conectores

En la mayoría de los casos, un administrador de cuentas de BlueXP necesitará poner en marcha un *Connector* en su red local o en la nube. El conector es un componente crucial para el uso diario de BlueXP. Permite a BlueXP gestionar los recursos y procesos de su entorno de cloud público.

Cuando se necesita un conector

Se necesita un conector para las siguientes funciones y servicios de BlueXP:

- Funciones de gestión de Amazon FSX para ONTAP
- Detección de Amazon S3
- Descubrimiento de Azure Blob
- Backup en el cloud
- Cloud Data SENSE
- Organización en niveles del cloud
- Cloud Volumes ONTAP
- Sistemas E-Series

- Caché de archivos global
- Descubrimiento de Google Cloud Storage
- Clústeres de Kubernetes
- Integración de clústeres de ONTAP en las instalaciones con servicios de datos de BlueXP
- StorageGRID

Se requiere un conector **not** para los siguientes servicios:

- Asesor digital

En casi todos los casos, puede añadir una licencia al monedero digital sin conector.

La única vez que se necesita un conector para agregar una licencia a la cartera digital es para licencias Cloud Volumes ONTAP *basadas en nodo*. En este caso, se requiere un conector porque los datos se toman de las licencias instaladas en los sistemas Cloud Volumes ONTAP.

- Creación de entornos de trabajo de Amazon FSX para ONTAP

Aunque no es necesario un conector para crear un entorno de trabajo, es necesario crear y gestionar volúmenes, replicar datos e integrar FSX para ONTAP con servicios de cloud de NetApp, como Data Sense y Cloud Sync.

- Azure NetApp Files

Aunque no es necesario un conector para configurar y gestionar Azure NetApp Files, se requiere un conector si desea utilizar Cloud Data Sense para analizar datos de Azure NetApp Files.

- Cloud Volumes Service para Google Cloud
- Cloud Sync
- Detección directa de clústeres de ONTAP en las instalaciones

Aunque no es necesario un conector para la detección directa de un clúster ONTAP en las instalaciones, se necesita un conector si desea aprovechar las características adicionales de BlueXP.

["Obtenga más información acerca de las opciones de detección y gestión para clústeres de ONTAP en las instalaciones"](#)

Ubicaciones admitidas

Se admite un conector en las siguientes ubicaciones:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- En sus instalaciones
- En sus instalaciones, sin acceso a Internet

Tenga nota sobre implementaciones de Azure

Si pone en marcha el conector en Azure, debe ponerse en marcha en la misma región de Azure que los

sistemas de Cloud Volumes ONTAP que gestiona o en ["Par de regiones de Azure"](#) Para los sistemas Cloud Volumes ONTAP. Este requisito garantiza que se utilice una conexión de enlace privado de Azure entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas. ["Conozca cómo Cloud Volumes ONTAP utiliza un enlace privado de Azure"](#).

Nota sobre implementaciones de Google Cloud

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.

Los conectores deben permanecer en funcionamiento

Un conector debe permanecer en funcionamiento en todo momento. Es importante para la salud y el funcionamiento continuos de los servicios que usted habilita.

Por ejemplo, un conector es un componente clave en el estado y la operación de Cloud Volumes ONTAP. Si el conector está apagado, los sistemas PAYGO de Cloud Volumes ONTAP y los sistemas BYOL basados en capacidad se apagan después de perder la comunicación con un conector durante más de 14 días. Esto sucede porque el conector actualiza las licencias del sistema cada día.



Si su sistema Cloud Volumes ONTAP tiene una licencia BYOL basada en nodos, el sistema seguirá ejecutándose transcurridos 14 días porque la licencia se instala en el sistema Cloud Volumes ONTAP.

BlueXP le notificará si su conector ha sido apagado durante 14 días o más. ["Más información sobre las notificaciones de BlueXP"](#).

Cómo crear un conector

Un administrador de cuentas de BlueXP puede crear un conector de varias maneras:

- Directamente de BlueXP (recomendado)
 - ["Cree en AWS"](#)
 - ["Cree en Azure"](#)
 - ["Crear en GCP"](#)
- Mediante la instalación manual del software en su propio host Linux
 - ["En un host que tiene acceso a Internet"](#)
 - ["En un host local que no tiene acceso a Internet"](#)
- Desde el mercado de su proveedor de cloud
 - ["Mercado AWS"](#)
 - ["Azure Marketplace"](#)

Si trabaja en una región gubernamental, necesita implementar un conector desde el mercado de su proveedor de cloud o instalar manualmente el software del conector en un host Linux existente. No puede desplegar el conector en una región gubernamental desde el sitio web de BlueXP SaaS.

Permisos

Se necesitan permisos específicos para crear el conector y se necesita otro conjunto de permisos para la propia instancia del conector.

Permisos para crear un conector

El usuario que crea un conector a partir de BlueXP necesita permisos específicos para implementar la instancia en su proveedor de cloud de elección.

- ["Consulte los permisos de AWS necesarios"](#)
- ["Consulte los permisos de Azure necesarios"](#)
- ["Consulte los permisos necesarios de Google Cloud"](#)

Permisos para la instancia de conector

El conector necesita permisos específicos de proveedor de cloud para realizar operaciones en su nombre. Por ejemplo, para poner en marcha y gestionar Cloud Volumes ONTAP.

Cuando crea un conector directamente desde BlueXP, BlueXP crea el conector con los permisos que necesita. No hay nada que usted necesita hacer.

Si crea el conector usted mismo desde AWS Marketplace, Azure Marketplace o mediante la instalación manual del software, tendrá que asegurarse de que cuenta con los permisos adecuados.

- ["Conozca cómo el conector utiliza los permisos de AWS"](#)
- ["Conozca cómo el conector utiliza los permisos de Azure"](#)
- ["Descubra cómo el conector utiliza los permisos de Google Cloud"](#)

Actualizaciones de conectores

Normalmente actualizamos el software del conector cada mes para introducir nuevas funciones y para proporcionar mejoras de estabilidad. Aunque la mayoría de los servicios y características de la plataforma BlueXP se ofrecen a través de software basado en SaaS, algunas características y funciones dependen de la versión del conector. Que incluye gestión de Cloud Volumes ONTAP, gestión de clústeres ONTAP en las instalaciones, configuración y ayuda.

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

Número de entornos de trabajo por conector

Un conector puede gestionar varios entornos de trabajo en BlueXP. El número máximo de entornos de trabajo que debe gestionar un único conector varía. Depende del tipo de entorno laboral, del número de volúmenes, de la cantidad de capacidad que se administra y del número de usuarios.

Si tiene una puesta en marcha a gran escala, trabaje con su representante de NetApp para dimensionar el entorno. Si experimenta algún problema a lo largo del camino, póngase en contacto con nosotros a través del chat en el producto.

Cuándo usar varios conectores

En algunos casos, es posible que sólo necesite un conector, pero es posible que necesite dos o más conectores.

A continuación, se muestran algunos ejemplos:

- Utiliza un entorno multicloud (AWS y Azure), por lo que tiene un conector en AWS y otro en Azure. Cada una de ellas gestiona los sistemas Cloud Volumes ONTAP que se ejecutan en estos entornos.

- Un proveedor de servicios puede utilizar una cuenta de NetApp para proporcionar servicios a sus clientes mientras utiliza otra cuenta para proporcionar recuperación ante desastres para una de sus unidades de negocio. Cada cuenta tendría conectores independientes.

Uso de varios conectores con el mismo entorno de trabajo

Puede gestionar un entorno de trabajo con varios conectores al mismo tiempo para fines de recuperación ante desastres. Si se cae un conector, puede cambiar al otro conector para gestionar inmediatamente el entorno de trabajo.

Para configurar esta configuración:

1. ["Cambie a otro conector"](#)
2. Detectar el entorno de trabajo existente.
 - ["Agregue sistemas Cloud Volumes ONTAP existentes a BlueXP"](#)
 - ["Detectar clústeres de ONTAP"](#)
3. Ajuste la ["Modo de gestión de la capacidad"](#)

Sólo el conector principal debe ajustarse en **modo automático**. Si cambia a otro conector para fines de DR, puede cambiar el modo de gestión de capacidad según sea necesario.

Cuándo cambiar entre conectores

Al crear el primer conector, BlueXP utiliza automáticamente ese conector para cada entorno de trabajo adicional que cree. Una vez creado un conector adicional, deberá cambiar entre ellos para ver los entornos de trabajo específicos de cada conector.

["Aprenda a cambiar entre conectores"](#).

La interfaz de usuario local

Mientras debe realizar casi todas las tareas de la ["Interfaz de usuario de SaaS"](#), una interfaz de usuario local todavía está disponible en el conector. Esta interfaz es necesaria si instala el conector en un entorno que no tiene acceso a Internet (como una región gubernamental) y para algunas tareas que se deben realizar desde el propio conector, en lugar de la interfaz SaaS:

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

["Aprenda a acceder a la interfaz de usuario local"](#).

Cree un conector en AWS desde BlueXP

Un administrador de cuentas de BlueXP necesita implementar un *Connector* antes de poder utilizar la mayoría de las funciones de BlueXP. Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público.

Estos pasos describen cómo crear un conector en una región comercial de AWS directamente desde el sitio web de BlueXP SaaS.

- ["Aprenda a desplegar un conector en una región gubernamental"](#)
- ["Obtenga información sobre otras formas de desplegar un conector"](#)

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1

Configure la autenticación

Para iniciar Connector en AWS, BlueXP debe autenticarse con AWS asumiendo un rol IAM o utilizando claves de acceso de AWS. Con cualquiera de las dos opciones, se requiere una política de IAM.

[Ver el rol IAM](#) o [siga las instrucciones paso a paso](#).

2

Configure las redes

Se necesita un VPC y una subred con acceso de salida a Internet hacia extremos específicos. Si se requiere un servidor proxy para Internet de salida, necesitará la dirección IP, las credenciales y el certificado HTTPS.

[Ver los requisitos de red](#).

3

Cree el conector

Haga clic en el menú desplegable conector, seleccione **Agregar conector** y siga las indicaciones.

[Siga las instrucciones paso a paso](#).

Configure la autenticación de AWS

BlueXP debe autenticarse con AWS para poder implementar la instancia de Connector en su VPC. Es posible elegir uno de los siguientes métodos de autenticación:

- Deje que BlueXP asuma una función de IAM que tenga los permisos necesarios
- Proporcione una clave secreta y de acceso de AWS para un usuario IAM que tenga los permisos necesarios

Con cualquiera de las dos opciones, primero debe empezar creando una política de IAM que incluya los permisos necesarios.

Cree una política de IAM

Esta directiva sólo contiene los permisos necesarios para iniciar la instancia de Connector en AWS desde BlueXP. No utilice esta política para otras situaciones.

Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos a la instancia de Connector que permite al conector administrar los recursos de su entorno de nube pública.

Pasos

1. Vaya a la consola IAM de AWS.

2. Haga clic en **Directivas > Crear directiva**.
3. Haga clic en **JSON**.
4. Copie y pegue la siguiente política:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:DeleteRole",
      "iam:PutRolePolicy",
      "iam:CreateInstanceProfile",
      "iam:DeleteRolePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam:DeleteInstanceProfile",
      "iam:PassRole",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:CreateSecurityGroup",
      "ec2:DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2:DescribeInstances",
      "ec2:CreateTags",
      "ec2:DescribeImages",
      "cloudformation:CreateStack",
      "cloudformation:DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
    ]
  }]
}
```

```

        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. Haga clic en **Siguiente** y agregue etiquetas, si es necesario.
6. Haga clic en **Siguiente** e introduzca un nombre y una descripción.
7. Haga clic en **Crear directiva**.

El futuro

Adjunte la política a una función de IAM que BlueXP puede asumir o a un usuario de IAM.

Configurar un rol de IAM

Configurar una función de IAM que BlueXP puede asumir para implementar Connector en AWS.

Pasos

1. Vaya a la consola AWS 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 de la cuenta de BlueXP SaaS: 952013314444

- Seleccione la directiva que ha creado en la sección anterior.

3. Después de crear la función, copie la función ARN para que pueda pegarla en BlueXP al crear el conector.

Resultado

El rol IAM ahora tiene los permisos necesarios.

Configurar permisos para un usuario de IAM

Al crear un conector, puede proporcionar una clave secreta y de acceso a AWS para un usuario IAM con los permisos necesarios para implementar la instancia del conector.

Pasos

1. En la consola AWS IAM, haga clic en **usuarios** y, a continuación, seleccione el nombre de usuario.
2. Haga clic en **Agregar permisos > Adjuntar directivas existentes directamente**.
3. Seleccione la política que ha creado.
4. Haga clic en **Siguiente** y, a continuación, en **Agregar permisos**.
5. Asegúrese de tener acceso a una clave de acceso y a una clave secreta para el usuario de IAM.

Resultado

Ahora el usuario de AWS tiene los permisos necesarios para crear el conector desde BlueXP. Deberá especificar las claves de acceso de AWS para este usuario cuando se le solicite BlueXP.

Configure las redes

Configure su red de modo que Connector pueda gestionar recursos y procesos en su entorno de cloud público. Además de tener una red virtual y una subred para el conector, deberá asegurarse de que se cumplen los siguientes requisitos.

Conexión a redes de destino


Un conector requiere una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que tiene previsto habilitar.

Por ejemplo, si instala un conector en su red corporativa, debe configurar una conexión VPN a la red virtual en la que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
https://<region>.amazonaws.com	Para gestionar recursos en AWS.
https://support.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.

Puntos finales	Específico
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	<p>Proporcionar funciones y servicios SaaS dentro de BlueXP.</p> <div>  <p>El conector se está comunicando actualmente con "cloudmanager.cloud.netapp.com" pero empezará a ponerse en contacto con "api.bluexp.netapp.com" en una próxima versión.</p> </div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	<p>Para actualizar el conector y sus componentes de Docker.</p>

Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico saliente de Internet, obtenga la siguiente información acerca del proxy HTTP o HTTPS:

- Dirección IP
- Credenciales
- Certificado HTTPS

Grupo de seguridad

No hay tráfico entrante en el conector, a menos que lo inicie o si el conector se utiliza como proxy para los mensajes AutoSupport. HTTP y HTTPS proporcionan acceso al ["Interfaz de usuario local"](#), que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

Limitación de dirección IP

Puede haber un conflicto con las direcciones IP en el rango 172. ["Obtenga más información sobre esta limitación"](#).

Cree un conector

BlueXP permite crear un conector en AWS directamente desde su interfaz de usuario.

Pasos

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Elija **Amazon Web Services** como su proveedor de cloud y haga clic en **continuar**.
3. En la página **despliegue de un conector**, revise los detalles sobre lo que necesitará. Dispone de dos opciones:
 - a. Haga clic en **continuar** para preparar la implementación utilizando la guía del producto. Cada paso de la guía del producto incluye la información que se incluye en esta página de la documentación.
 - b. Haga clic en **Ir a implementación** si ya ha preparado siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el conector:
 - **Prepárese**: Revise lo que necesitará.
 - **Credenciales de AWS**: Especifique su región de AWS y, a continuación, elija un método de autenticación, que es una función de IAM que BlueXP puede asumir o una clave de acceso y clave secreta de AWS.



Si elige **asumir función**, puede crear el primer conjunto de credenciales desde el asistente de implementación del conector. Debe crear cualquier conjunto adicional de credenciales desde la página Credentials. A continuación, estarán disponibles en el asistente en una lista desplegable. ["Aprenda a añadir credenciales adicionales"](#).

- **Detalles**: Proporcione detalles sobre el conector.
 - Escriba un nombre para la instancia.
 - Añada etiquetas personalizadas (metadatos) a la instancia.
 - Elija si desea que BlueXP cree una nueva función que tenga los permisos necesarios o si desea seleccionar una función existente con la que haya configurado ["los permisos necesarios"](#).
 - Elija si desea cifrar los discos EBS del conector. Tiene la opción de utilizar la clave de cifrado predeterminada o utilizar una clave personalizada.
- **Red**: Especifique un VPC, una subred y un par de claves para la instancia, elija si desea habilitar una dirección IP pública y, opcionalmente, especifique una configuración de proxy (se admiten HTTP y HTTPS).

Asegúrese de que tiene el par de llaves correcto para usar con el conector. Sin un par de teclas, no podrá acceder a la máquina virtual conector.

- **Grupo de seguridad**: Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.
- **Revisión**: Revise sus selecciones para verificar que su configuración es correcta.

5. Haga clic en **Agregar**.

La instancia debe estar lista en unos 7 minutos. Debe permanecer en la página hasta que el proceso se complete.

Después de terminar

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"](#).

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 en Azure desde BlueXP

Un administrador de cuentas de BlueXP necesita implementar un *Connector* antes de poder utilizar la mayoría de las funciones de BlueXP. Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público.

Estos pasos describen cómo crear un conector en una región comercial de Azure directamente desde el sitio web de SaaS de BlueXP.

- ["Aprenda a desplegar un conector en una región gubernamental"](#)
- ["Obtenga información sobre otras formas de desplegar un conector"](#)

Descripción general

Para implementar un conector, debe proporcionar a BlueXP un inicio de sesión que tenga los permisos necesarios para crear el conector VM en Azure.

Dispone de dos opciones:

1. Inicie sesión con su cuenta de Microsoft cuando se le solicite. Esta cuenta debe tener permisos de Azure específicos. Esta es la opción predeterminada.

[Siga los pasos que aparecen a continuación para comenzar.](#)

2. Proporcionar detalles acerca de un director de servicio de Azure AD. Este principal de servicio también requiere permisos específicos.

[Siga los pasos que aparecen a continuación para comenzar.](#)

Nota sobre las regiones de Azure

El conector debe ponerse en marcha en la misma región de Azure que los sistemas Cloud Volumes ONTAP que gestione o en ["Par de regiones de Azure"](#) Para los sistemas Cloud Volumes ONTAP. Este requisito garantiza que se utilice una conexión de enlace privado de Azure entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas.

["Conozca cómo Cloud Volumes ONTAP utiliza un enlace privado de Azure"](#)

Configure las redes

Configure su red de modo que Connector pueda gestionar recursos y procesos en su entorno de cloud público. Además de tener una red virtual y una subred para el conector, deberá asegurarse de que se cumplen los siguientes requisitos.


Conexión a redes de destino

Un conector requiere una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que tiene previsto habilitar.

Por ejemplo, si instala un conector en su red corporativa, debe configurar una conexión VPN a la red virtual en la que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com	Para gestionar recursos en regiones públicas de Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us	Para gestionar recursos en regiones gubernamentales de Azure.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud	Para administrar recursos en la región de Azure IL6.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://support.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	<div> El conector se está comunicando actualmente con "cloudmanager.cloud.netapp.com" pero empezará a ponerse en contacto con "api.blueexp.netapp.com" en una próxima versión.</div>

Puntos finales	Específico
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Para actualizar el conector y sus componentes de Docker.

Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico saliente de Internet, obtenga la siguiente información acerca del proxy HTTP o HTTPS:

- Dirección IP
- Credenciales
- Certificado HTTPS

Grupo de seguridad

No hay tráfico entrante en el conector, a menos que lo inicie o si el conector se utiliza como proxy para los mensajes AutoSupport. HTTP y HTTPS proporcionan acceso al ["Interfaz de usuario local"](#), que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

Limitación de dirección IP

Puede haber un conflicto con las direcciones IP en el rango 172. ["Obtenga más información sobre esta limitación"](#).

Cree un conector con su cuenta de Azure

La forma predeterminada de crear un conector en Azure es iniciar sesión con su cuenta de Azure cuando se le solicite. El formulario de inicio de sesión es propiedad de Microsoft y está alojado en él. Sus credenciales no se proporcionan a NetApp.

Configure permisos para la cuenta de Azure

Antes de implementar un conector desde BlueXP, debe asegurarse de que su cuenta de Azure tenga los permisos correctos.

Pasos

1. Copie los permisos necesarios para un nuevo rol personalizado en Azure y guárdelo en un archivo JSON.



Esta política solo contiene los permisos necesarios para iniciar Connector VM en Azure desde BlueXP. No utilice esta política para otras situaciones. Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos al conector VM que permite al conector administrar los recursos de su entorno de nube pública.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
```

```

"Microsoft.Compute/operations/read",
"Microsoft.Compute/virtualMachines/instanceView/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/availabilitySets/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
"Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",

```

```

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
],
"NotActions": [],
"AssignableScopes": [],
"Description": "Azure SetupAsService",
"IsCustom": "true"
}

```

2. Modifique el JSON añadiendo su ID de suscripción de Azure al ámbito asignable.

ejemplo

```

"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

3. 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.

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



c. Introduzca el siguiente comando CLI de Azure:

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

Ahora debería tener una función personalizada denominada *Azure SetupAsService*.

4. Asigne la función al usuario que implementará Connector desde BlueXP:
 - a. Abra el servicio **Suscripciones** y seleccione la suscripción del usuario.
 - b. Haga clic en **Control de acceso (IAM)**.
 - c. Haga clic en **Agregar > Agregar asignación de rol** y, a continuación, agregue los permisos:
 - Seleccione el rol **Azure SetupAsService** y haga clic en **Siguiente**.



Azure SetupAsService es el nombre predeterminado proporcionado en la política de implementación de Connector para Azure. Si seleccionó otro nombre para el rol, seleccione ese nombre.

- Mantener seleccionado **Usuario, grupo o principal de servicio**.
- Haga clic en **Seleccionar miembros**, elija su cuenta de usuario y haga clic en **Seleccionar**.
- Haga clic en **Siguiente**.
- Haga clic en **revisar + asignar**.

Resultado

El usuario de Azure ahora tiene los permisos necesarios para implementar Connector desde BlueXP.

Cree el conector iniciando sesión con su cuenta de Azure

BlueXP permite crear un conector en Azure directamente desde su interfaz de usuario.

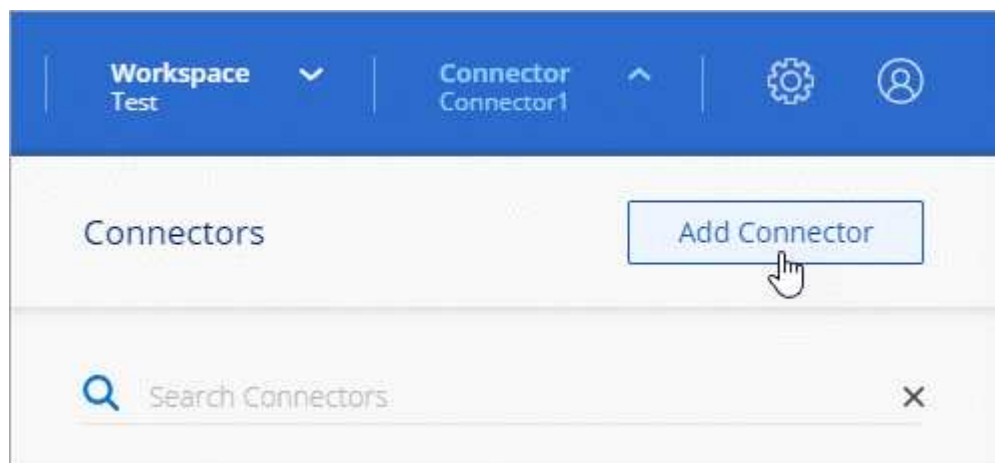
Lo que necesitará

- Una suscripción a Azure.
- Una red virtual y una subred en su región de Azure preferida.
- Si no quiere que BlueXP cree automáticamente una función de Azure para Connector, tendrá que crear la suya propia ["uso de la política en esta página"](#).

Estos permisos son para la propia instancia de Connector. Se trata de un conjunto de permisos diferente al que se configuró anteriormente para desplegar el conector.

Pasos

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Elija **Microsoft Azure** como proveedor de cloud.
3. En la página **despliegue de un conector**, revise los detalles sobre lo que necesitará. Dispone de dos opciones:
 - a. Haga clic en **continuar** para preparar la implementación utilizando la guía del producto. Cada paso incluye información contenida en esta página de la documentación.
 - b. Haga clic en **Ir a implementación** si ya ha preparado siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el conector:
 - Si se le solicita, inicie sesión en su cuenta de Microsoft, que debería tener los permisos necesarios para crear la máquina virtual.

El formulario es propiedad de Microsoft y está alojado en él. Sus credenciales no se proporcionan a NetApp.



Si ya ha iniciado sesión en una cuenta de Azure, BlueXP utilizará esa cuenta automáticamente. Si tiene varias cuentas, es posible que deba cerrar la sesión primero para asegurarse de utilizar la cuenta correcta.

- **Autenticación de VM:** Elija una suscripción de Azure, una ubicación, un nuevo grupo de recursos o un grupo de recursos existente y, a continuación, elija un método de autenticación.
- **Detalles:** Escriba un nombre para la instancia, especifique etiquetas y elija si desea que BlueXP cree una nueva función que tenga los permisos necesarios o si desea seleccionar una función existente con la que se haya configurado ["los permisos necesarios"](#).

Tenga en cuenta que puede elegir las suscripciones asociadas a esta función. Cada suscripción que elija proporciona al conector permisos para implementar Cloud Volumes ONTAP en esas suscripciones.

- **Red:** Elija un vnet y una subred, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
- **Grupo de seguridad:** Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.
- **Revisión:** Revise sus selecciones para verificar que su configuración es correcta.

5. Haga clic en **Agregar**.

La máquina virtual debe estar lista en unos 7 minutos. Debe permanecer en la página hasta que el proceso se complete.

Después de terminar

Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP. 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. ["Leer más"](#).

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"](#).

Cree un conector con un director de servicio

En lugar de iniciar sesión con su cuenta de Azure, también tiene la opción de proporcionar a BlueXP las credenciales de una entidad de servicio de Azure que tenga los permisos necesarios.

Concesión de permisos de Azure con un director de servicio

Conceda los permisos necesarios para implementar un conector en Azure mediante la creación y configuración de un servicio principal en Azure Active Directory y la obtención de las credenciales de Azure que BlueXP necesita.

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](#).

Cree una aplicación de Azure Active Directory

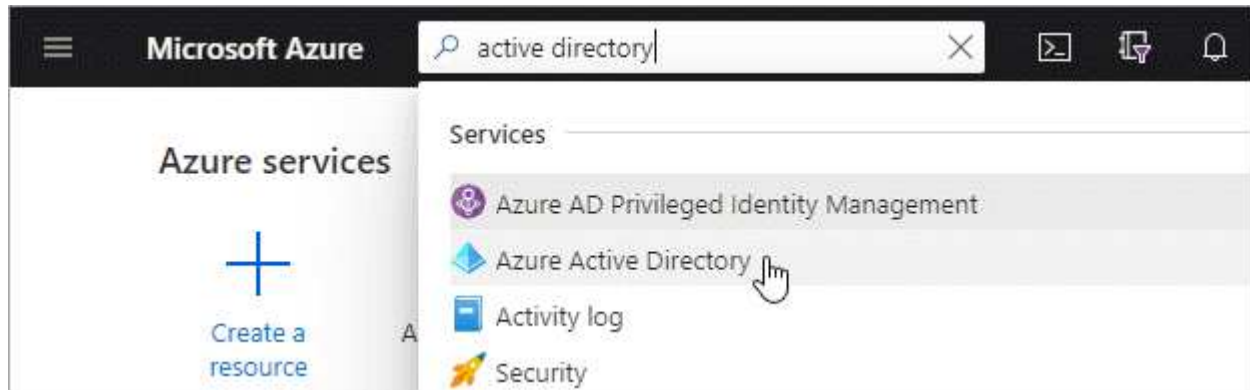
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que BlueXP pueda utilizar para implementar Connector.

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.

Asigne la aplicación a una función

Debe enlazar la entidad de servicio a la suscripción a Azure en la que planea implementar el conector y asignarle el rol personalizado "Azure SetupAsService".

Pasos

1. Copie los permisos necesarios para un nuevo rol personalizado en Azure y guárdelo en un archivo JSON.



Esta política solo contiene los permisos necesarios para iniciar Connector VM en Azure desde BlueXP. No utilice esta política para otras situaciones. Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos al conector VM que permite al conector administrar los recursos de su entorno de nube pública.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
```

```
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/availabilitySets/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
"Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
```

```

        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

        "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

        "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}

```

2. Modifique el archivo JSON añadiendo su ID de suscripción de Azure al ámbito asignable.

ejemplo

```

"AssignableScopes": [
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]

```

3. 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.

- a. Comenzar "[Shell de cloud de Azure](#)" Y seleccione el entorno Bash.
- b. Cargue el archivo JSON.



c. Introduzca el siguiente comando CLI de Azure:

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

Ahora debería tener una función personalizada denominada *Azure SetupAsService*.

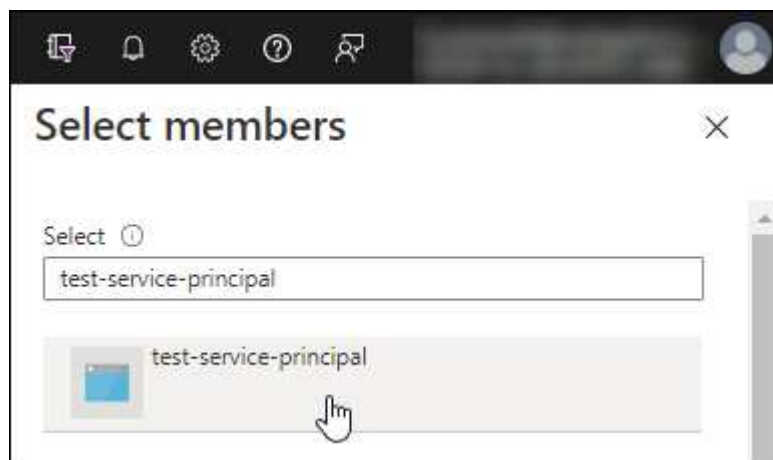
4. Asigne la aplicación al rol:

- 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 **Azure SetupAsService** 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**.
 - a. Haga clic en **revisar + asignar**.

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

Añada 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.

 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 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](#)

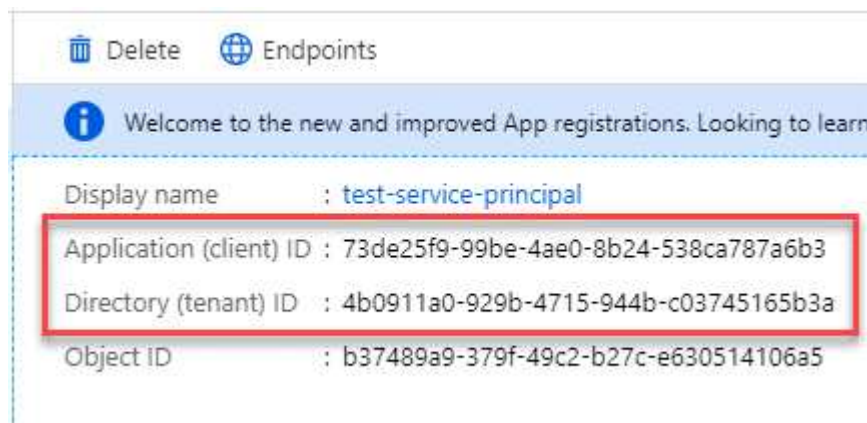
<input type="text" value="Type to search"/>	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

Obtener el ID de aplicación y el ID de directorio

Al crear el conector desde BlueXP, debe proporcionar el ID de aplicación (cliente) y el ID de directorio (arrendatario) 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)**.



Cree 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. Debe introducir esta información en BlueXP cuando cree el conector.

Cree el conector iniciando sesión con el principal de servicio

BlueXP permite crear un conector en Azure directamente desde su interfaz de usuario.

Lo que necesitará

- Una suscripción a Azure.
- Una red virtual y una subred en su región de Azure preferida.
- Detalles sobre un servidor proxy, si su empresa requiere un proxy para todo el tráfico saliente de Internet:
 - Dirección IP
 - Credenciales
 - Certificado HTTPS
- Si no quiere que BlueXP cree automáticamente una función de Azure para Connector, tendrá que crear la suya propia ["uso de la política en esta página"](#).

Estos permisos son para la propia instancia de Connector. Se trata de un conjunto de permisos diferente al que se configuró anteriormente para desplegar el conector.

Pasos

- Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Elija **Microsoft Azure** como proveedor de cloud.
3. En la página **despliegue de un conector**:
 - a. En **autenticación**, haga clic en **principal de servicio de Active Directory** e introduzca información acerca del principal de servicio de Azure Active Directory que concede los permisos necesarios:
 - ID de aplicación (cliente): Consulte [Obtener el ID de aplicación y el ID de directorio](#).
 - ID de directorio (arrendatario): Consulte [Obtener el ID de aplicación y el ID de directorio](#).
 - Client Secret: Consulte [Cree un secreto de cliente](#).
 - b. Haga clic en **Iniciar sesión**.
 - c. Ahora tiene dos opciones:
 - Haga clic en **continuar** para preparar la implementación utilizando la guía del producto. Cada paso de la guía del producto incluye la información que se incluye en esta página de la documentación.
 - Haga clic en **Ir a implementación** si ya ha preparado siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el conector:
 - **Autenticación de VM**: Elija una suscripción de Azure, una ubicación, un nuevo grupo de recursos o un grupo de recursos existente y, a continuación, elija un método de autenticación.
 - **Detalles**: Escriba un nombre para la instancia, especifique etiquetas y elija si desea que BlueXP cree una nueva función que tenga los permisos necesarios o si desea seleccionar una función existente con la que se haya configurado "[los permisos necesarios](#)".

Tenga en cuenta que puede elegir las suscripciones asociadas a esta función. Cada suscripción que elija proporciona al conector permisos para implementar Cloud Volumes ONTAP en esas suscripciones.
 - **Red**: Elija un vnet y una subred, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
 - **Grupo de seguridad**: Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.
 - **Revisión**: Revise sus selecciones para verificar que su configuración es correcta.
5. Haga clic en **Agregar**.

La máquina virtual debe estar lista en unos 7 minutos. Debe permanecer en la página hasta que el proceso se complete.

Después de terminar

Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP. 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. ["Leer más"](#).

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.

Crear un conector en Google Cloud desde BlueXP

Un administrador de cuentas de BlueXP necesita implementar un *Connector* antes de poder utilizar la mayoría de las funciones de BlueXP. ["Aprender cuando se necesita un conector"](#). Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público.

Esta página describe cómo crear un conector en Google Cloud directamente desde BlueXP. ["Obtenga información sobre otras formas de desplegar un conector"](#).

Estos pasos deben ser completados por un usuario que tenga la función de administrador de cuentas. Un administrador de área de trabajo no puede crear un conector.



Al crear su primer entorno de trabajo de Cloud Volumes ONTAP, BlueXP le solicitará que cree un conector si aún no lo tiene.

Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.



Configure los permisos

- Asegúrese de que su cuenta de Google Cloud tiene los permisos correctos creando y adjuntando una función personalizada.

[Configure los permisos para desplegar el conector.](#)

- Al crear el conector VM, debe asociarlo con una cuenta de servicio. Esta cuenta de servicio debe tener una función personalizada con permisos para gestionar recursos en Google Cloud.

[Configure una cuenta de servicio para el conector.](#)

- Si va a implementar Cloud Volumes ONTAP en varios proyectos, asegúrese de que el conector tiene acceso a dichos proyectos.

[Configure permisos en todos los proyectos.](#)

- Si utiliza un VPC compartido, configure los permisos en el proyecto de servicio y en el proyecto de host.

[Configure los permisos VPC compartidos.](#)

2

Configure las redes

Se necesita un VPC y una subred con acceso de salida a Internet hacia extremos específicos. Si se requiere un servidor proxy para Internet de salida, necesitará la dirección IP, las credenciales y el certificado HTTPS.

[Ver los requisitos de red.](#)

3

Habilite las API de Google Cloud

- API de Cloud Deployment Manager V2
- API de registro en la nube
- API de Cloud Resource Manager
- API del motor de computación
- API de gestión de acceso e identidad (IAM)

4

Cree el conector

Haga clic en el menú desplegable conector, seleccione **Agregar conector** y siga las indicaciones.

[Siga las instrucciones paso a paso.](#)

Configure los permisos

Se requieren permisos para lo siguiente:

- El usuario que desplegará el conector VM
- Una cuenta de servicio que necesita conectar a la máquina virtual del conector durante la implementación

Según la configuración existente, es posible que deba realizar también los siguientes pasos:

- Configure permisos en todos los proyectos
- Configurar permisos para un VPC compartido

Configure los permisos para desplegar el conector

Antes de implementar un conector, debe asegurarse de que su cuenta de Google Cloud tiene los permisos correctos.

Pasos

1. "Crear una función personalizada" esto incluye los siguientes permisos:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
```

- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `resourcemanager.projects.get`
- `compute.instances.setServiceAccount`
- `iam.serviceAccounts.list`

2. Adjunte la función personalizada al usuario que implementará Connector desde BlueXP.

Resultado

Ahora el usuario de Google Cloud tiene los permisos necesarios para crear el conector.

Configure una cuenta de servicio para el conector

Se requiere una cuenta de servicio para proporcionar al conector el permiso que necesita para gestionar recursos en Google Cloud. Asociará esta cuenta de servicio con el conector VM al crearla.

Los permisos para la cuenta de servicio son diferentes a los permisos que configuró en la sección anterior.

Pasos

1. "Crear una función personalizada" esto incluye los siguientes permisos:

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
```


- `compute.networks.updatePolicy`
- `compute.backendServices.create`
- `compute.addresses.list`
- `compute.disks.create`
- `compute.disks.createSnapshot`
- `compute.disks.delete`
- `compute.disks.get`
- `compute.disks.list`
- `compute.disks.setLabels`
- `compute.disks.use`
- `compute.firewalls.create`
- `compute.firewalls.delete`
- `compute.firewalls.get`
- `compute.firewalls.list`
- `compute.globalOperations.get`
- `compute.images.get`
- `compute.images.getFromFamily`
- `compute.images.list`
- `compute.images.useReadOnly`
- `compute.instances.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.instanceGroups.get`
- `compute.addresses.get`
- `compute.instances.updateNetworkInterface`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`

- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `compute.instances.setServiceAccount`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `logging.logEntries.list`
- `logging.privateLogEntries.list`
- `resourcemanager.projects.get`
- `storage.buckets.create`
- `storage.buckets.delete`
- `storage.buckets.get`
- `storage.buckets.list`
- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`
- `storage.buckets.update`
- `iam.serviceAccounts.getIamPolicy`
- `iam.serviceAccounts.list`
- `storage.objects.get`
- `storage.objects.list`
- `monitoring.timeSeries.list`
- `storage.buckets.getIamPolicy`
- `cloudkms.cryptoKeys.getIamPolicy`

- `cloudkms.cryptoKeys.setIamPolicy`
- `cloudkms.keyRings.get`
- `cloudkms.keyRings.getIamPolicy`
- `cloudkms.keyRings.setIamPolicy`

2. "Cree una cuenta de servicio de Google Cloud y aplique la función personalizada que acaba de crear".
3. 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.

Resultado

Se ha configurado la cuenta de servicio del conector VM.

Configure permisos en todos los proyectos

Si planea implementar sistemas Cloud Volumes ONTAP en proyectos diferentes a los del proyecto en el que reside el conector, tendrá que proporcionar a la cuenta de servicio del conector acceso a dichos proyectos.

Por ejemplo, supongamos que el conector está en el proyecto 1 y que desea crear sistemas Cloud Volumes ONTAP en el proyecto 2. Tendrá que otorgar acceso a la cuenta de servicio en el proyecto 2.

Pasos

1. En la consola de Google Cloud, vaya al servicio IAM y seleccione el proyecto en el que desea crear sistemas Cloud Volumes ONTAP.
2. En la página **IAM**, seleccione **conceder acceso** y proporcione la información necesaria.
 - Introduzca el correo electrónico de la cuenta de servicio del conector.
 - Seleccione el rol personalizado del conector.
 - Haga clic en **Guardar**.

Para obtener información detallada, consulte "[Documentación de Google Cloud](#)"

Configure los permisos VPC compartidos

Si se utiliza un VPC compartido para implementar recursos en un proyecto de servicio, se requieren los siguientes permisos. Esta tabla es de referencia y el entorno debe reflejar la tabla de permisos cuando se haya completado la configuración de IAM.

Identidad	Creador	Alojadas en	Permisos de proyecto de servicio	Permisos del proyecto host	Específico
Cuenta de Google utilizada para desplegar el conector	Personalizado	Proyecto de servicio	<ul style="list-style-type: none"> • "Los permisos encontrados en esta sección anterior" 	<ul style="list-style-type: none"> • compute.networkUser 	Despliegue del conector en el proyecto de servicio

Identidad	Creador	Alojadas en	Permisos de proyecto de servicio	Permisos del proyecto host	Específico
Cuenta de servicio del conector	Personalizado	Proyecto de servicio	<ul style="list-style-type: none"> • "Los permisos encontrados en esta sección anterior" 	<ul style="list-style-type: none"> • compute.networkUser • deploymentmanager.editor 	Implementación y mantenimiento de Cloud Volumes ONTAP y servicios en el proyecto de servicio
Cuenta de servicio de Cloud Volumes ONTAP	Personalizado	Proyecto de servicio	<ul style="list-style-type: none"> • storage.admin • miembro: Cuenta de servicio de BlueXP como serviceAccount.user 	N.A.	(Opcional) para la organización en niveles de datos y Cloud Backup
Agente de servicio de API de Google	Google Cloud	Proyecto de servicio	<ul style="list-style-type: none"> • (Predeterminado) Editor 	<ul style="list-style-type: none"> • compute.networkUser 	Interactúa con las API de Google Cloud en nombre de la implementación. Permite a BlueXP utilizar la red compartida.
Cuenta de servicio predeterminada de Google Compute Engine	Google Cloud	Proyecto de servicio	<ul style="list-style-type: none"> • (Predeterminado) Editor 	<ul style="list-style-type: none"> • compute.networkUser 	Pone en marcha instancias de Google Cloud e infraestructura de computación en nombre de la puesta en marcha. Permite a BlueXP utilizar la red compartida.

Notas:

1. deploymentmanager.editor sólo es necesario en el proyecto host si no pasa reglas de firewall a la implementación y decide dejar que BlueXP las cree por usted. BlueXP creará una implementación en el proyecto host que contiene la regla de firewall VPC0 si no se especifica ninguna regla.
2. Firewall.create y firewall.delete sólo son necesarios si no está pasando reglas de firewall a la implementación y está eligiendo permitir que BlueXP las cree para usted. Estos permisos residen en el archivo .yaml de cuenta de BlueXP. Si va a implementar un par de alta disponibilidad mediante un VPC compartido, estos permisos se utilizarán para crear las reglas de firewall para VPC1, 2 y 3. Para todas las demás implementaciones, estos permisos también se utilizarán para crear reglas para VPC0.
3. Para la organización en niveles de los datos, la cuenta del servicio de organización en niveles debe tener el rol serviceAccount.user en la cuenta de servicio, no solo en el nivel del proyecto. Actualmente, si asigna serviceAccount.user en el nivel de proyecto, los permisos no se muestran cuando consulta la cuenta de servicio con getIAMPolicy.

Configure las redes

Configure su red de modo que Connector pueda gestionar recursos y procesos en su entorno de cloud público. Además de tener una red virtual y una subred para el conector, deberá asegurarse de que se cumplen los siguientes requisitos.

Conexión a redes de destino

Un conector requiere una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que tiene previsto habilitar.

Por ejemplo, si instala un conector en su red corporativa, debe configurar una conexión VPN a la red virtual en la que inicie Cloud Volumes ONTAP.

Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
https://www.googleapis.com/compute/v1/ https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Para gestionar recursos en Google Cloud.
https://support.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	<div><div>Proporcionar funciones y servicios SaaS dentro de BlueXP.</div><div><div>El conector se está comunicando actualmente con "cloudmanager.cloud.netapp.com" pero empezará a ponerse en contacto con "api.bluexp.netapp.com" en una próxima versión.</div></div></div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Para actualizar el conector y sus componentes de Docker.

Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico saliente de Internet, obtenga la siguiente información acerca del proxy HTTP o HTTPS:

- Dirección IP
- Credenciales

- Certificado HTTPS

Grupo de seguridad

No hay tráfico entrante en el conector, a menos que lo inicie o si el conector se utiliza como proxy para los mensajes AutoSupport. HTTP y HTTPS proporcionan acceso al ["Interfaz de usuario local"](#), que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

Limitación de dirección IP

Puede haber un conflicto con las direcciones IP en el rango 172. ["Obtenga más información sobre esta limitación"](#).

Habilite las API de Google Cloud

Se necesitan varias API para implementar el conector y Cloud Volumes ONTAP.

Paso

1. ["Habilite las siguientes API de Google Cloud en su proyecto"](#).
 - API de Cloud Deployment Manager V2
 - API de registro en la nube
 - API de Cloud Resource Manager
 - API del motor de computación
 - API de gestión de acceso e identidad (IAM)

Cree un conector

Cree un conector en Google Cloud directamente desde la interfaz de usuario de BlueXP o utilizando gcloud.

BlueXP

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Elija **Google Cloud Platform** como su proveedor de cloud.
3. En la página **despliegue de un conector**, revise los detalles sobre lo que necesitará. Dispone de dos opciones:
 - a. Haga clic en **continuar** para preparar la implementación utilizando la guía del producto. Cada paso de la guía del producto incluye la información que se incluye en esta página de la documentación.
 - b. Haga clic en **Ir a implementación** si ya ha preparado siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el conector:
 - Si se le solicita, inicie sesión en su cuenta de Google, que debería tener los permisos necesarios para crear la instancia de la máquina virtual.

El formulario es propiedad de Google y está alojado en él. Sus credenciales no se proporcionan a NetApp.

- **Detalles:** Introduzca un nombre para la instancia de la máquina virtual, especifique etiquetas, seleccione un proyecto y, a continuación, seleccione la cuenta de servicio que tenga los permisos necesarios (consulte la sección anterior para obtener más información).
 - **ubicación:** Especifique una región, zona, VPC y subred para la instancia.
 - **Red:** Elija si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
 - **Directiva de firewall:** Elija si desea crear una nueva directiva de firewall o si desea seleccionar una directiva de firewall existente que permita el acceso entrante HTTP, HTTPS y SSH.
 - **Revisión:** Revise sus selecciones para verificar que su configuración es correcta.
5. Haga clic en **Agregar**.

La instancia debe estar lista en unos 7 minutos. Debe permanecer en la página hasta que el proceso se complete.

1. Inicie sesión en el SDK de gcloud con su metodología preferida.

En nuestros ejemplos, utilizaremos un shell local con gcloud SDK instalado, pero puede utilizar Google Cloud Shell nativo en la consola de Google Cloud.

Para obtener más información acerca de Google Cloud SDK, visite la ["Página de documentación de Google Cloud SDK"](#).

2. Compruebe que ha iniciado sesión como usuario que tiene los permisos necesarios definidos en la sección anterior:

```
gcloud auth list
```

El resultado debe mostrar lo siguiente en el que la cuenta de usuario * es la cuenta de usuario que desea iniciar sesión como:

```
Credentialed Accounts
ACTIVE  ACCOUNT
      some_user_account@domain.com
*      desired_user_account@domain.com
To set the active account, run:
$ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Ejecute el `gcloud compute instances create` comando:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```


nombre-instancia

El nombre de la instancia de máquina virtual que desee para la instancia de.

proyecto

(Opcional) el proyecto en el que desea poner en marcha la máquina virtual.

cuenta de servicio

La cuenta de servicio especificada en la salida del paso 2.

zona

La zona en la que desea implementar la máquina virtual

sin dirección

(Opcional) no se utiliza ninguna dirección IP externa (se necesita un NAT o un proxy en la nube para enrutar el tráfico a Internet pública)

etiqueta de red

(Opcional) Agregar etiquetado de red para vincular una regla de firewall mediante etiquetas a la instancia de conector

ruta de la red

(Opcional) Añada el nombre de la red a la cual implementar el conector en (para un VPC compartido, se necesita la ruta completa)

ruta de subred

(Opcional) Añada el nombre de la subred en la que se va a implementar el conector (para un VPC compartido, se necesita la ruta completa)

km-clave-ruta

(Opcional) Agregar una clave KMS para cifrar los discos del conector (también es necesario aplicar permisos IAM)

Para obtener más información acerca de estas marcas, visite ["Documentación sobre Google Cloud Computing SDK"](#).

+

Al ejecutar el comando se pone en marcha el conector con la imagen maestra de NetApp. La instancia y el software del conector deben estar funcionando en aproximadamente cinco minutos.

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

`https://ipaddress[]`

2. 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. 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 de Google Cloud Storage en la misma cuenta de Google Cloud en la que creó el conector, verá que aparece un entorno de trabajo de Google Cloud Storage 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.

Cree un conector en una región gubernamental

Si trabaja en una región gubernamental, necesita implementar un conector desde el mercado de su proveedor de cloud o instalar manualmente el software del conector en un host Linux existente. No puede desplegar el conector en una región gubernamental desde el sitio web de BlueXP SaaS.

Utilice uno de los siguientes vínculos para ver las instrucciones para crear un conector:

- ["Cree un conector desde AWS Marketplace"](#)
- ["Cree un conector y un Cloud Volumes ONTAP en el entorno AWS C2S"](#)
- ["Cree un conector desde Azure Marketplace"](#)
- ["Instale un conector en su propio host Linux"](#)

Para las instalaciones manuales en su propio host Linux, debe utilizar el instalador "online" para instalar el conector en un host que tenga acceso a Internet. Hay disponible un instalador independiente "offline" para el conector, pero sólo es compatible con sitios locales que no tienen acceso a Internet. No cuenta con soporte para regiones gubernamentales.

Después de desplegar el conector, puede acceder a BlueXP abriendo el explorador Web y conectándose a la dirección IP de la instancia de conector: `https://ipaddress[]`

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

A continuación, ¿dónde ir

Ahora que ha iniciado sesión y configurado BlueXP, los usuarios pueden comenzar a

crear y descubrir entornos de trabajo.

- ["Azure NetApp Files"](#)
- ["Amazon FSX para ONTAP"](#)
- ["Cloud Volumes ONTAP para AWS"](#)
- ["Cloud Volumes ONTAP para Azure"](#)
- ["Cloud Volumes ONTAP para Google Cloud"](#)
- ["Cloud Volumes Service para Google Cloud"](#)
- ["Sistemas E-Series"](#)
- ["Clústeres de Kubernetes"](#)
- ["Clústeres de ONTAP en las instalaciones"](#)
- ["Sistemas StorageGRID"](#)

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

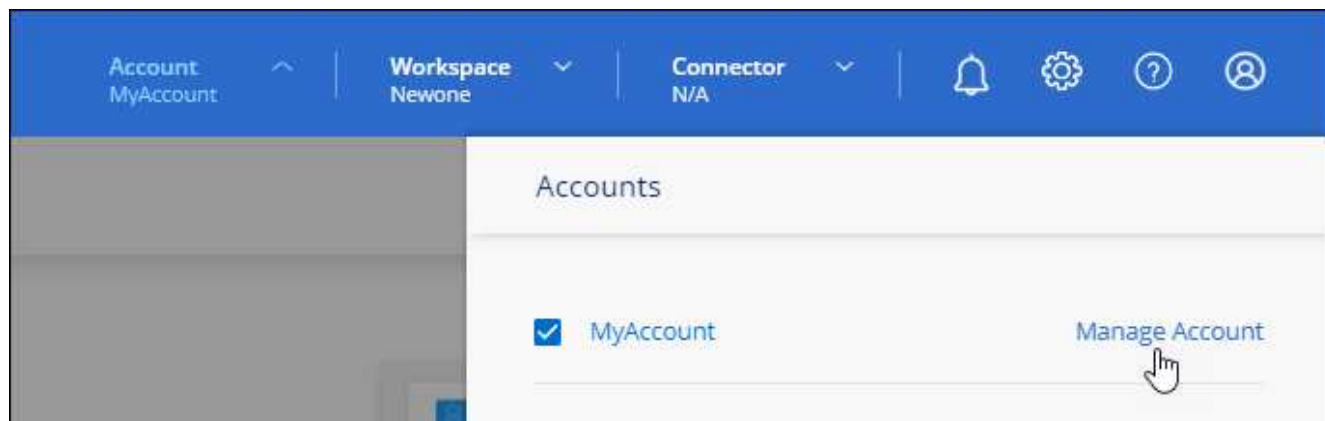
Asocie los usuarios con su cuenta de NetApp para que esos usuarios puedan crear y gestionar entornos de trabajo en BlueXP.

Pasos

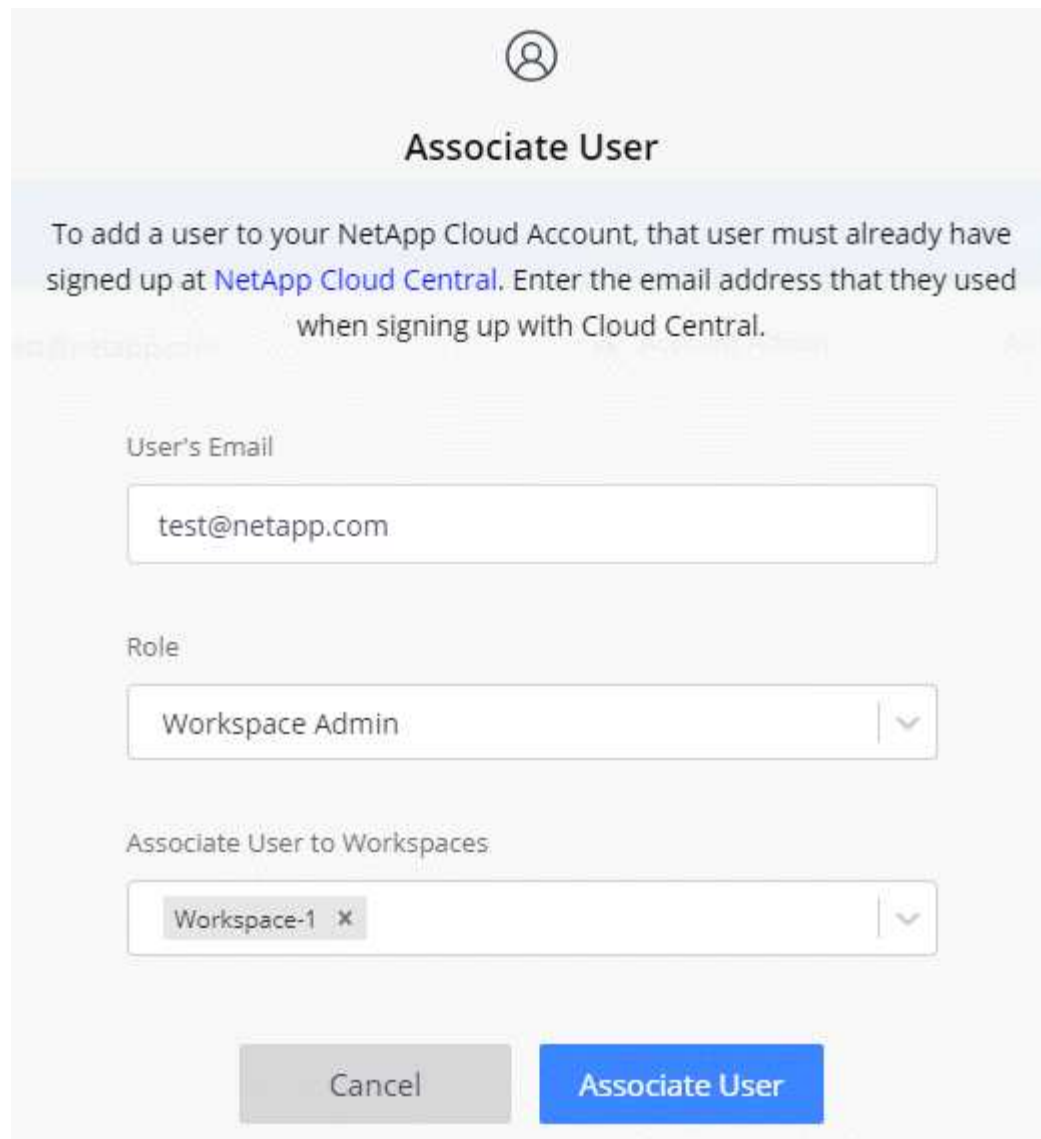
1. Si el usuario aún no lo ha hecho, pida al usuario que vaya a. "[Sitio web de NetApp BlueXP](#)" y regístrese.
2. En la parte superior de BlueXP, haga clic en el menú desplegable **cuenta**.




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 to add a user from NetApp Cloud Central. There are three input fields: "User's Email" with the value "test@netapp.com", "Role" with the value "Workspace Admin", and "Associate User to Workspaces" with the value "Workspace-1". 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

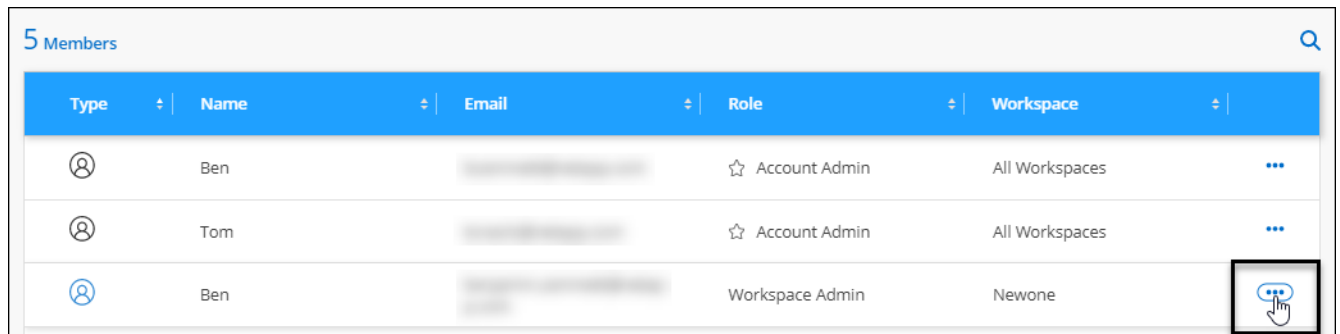
Desasociar un usuario hace que pueda dejar de acceder a los recursos de una cuenta de NetApp.

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

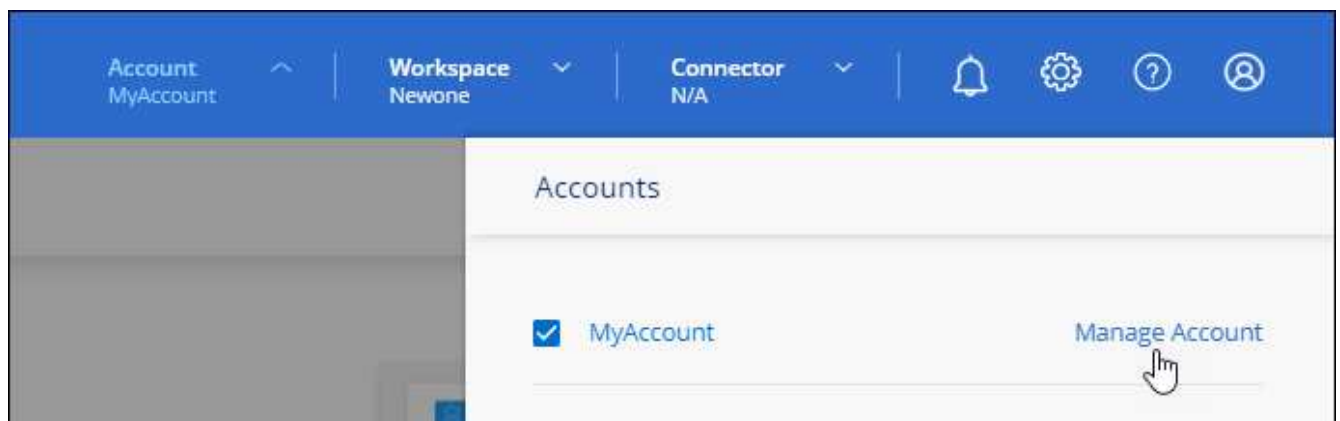
El usuario ya no puede acceder a los recursos de esta cuenta de NetApp.

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.

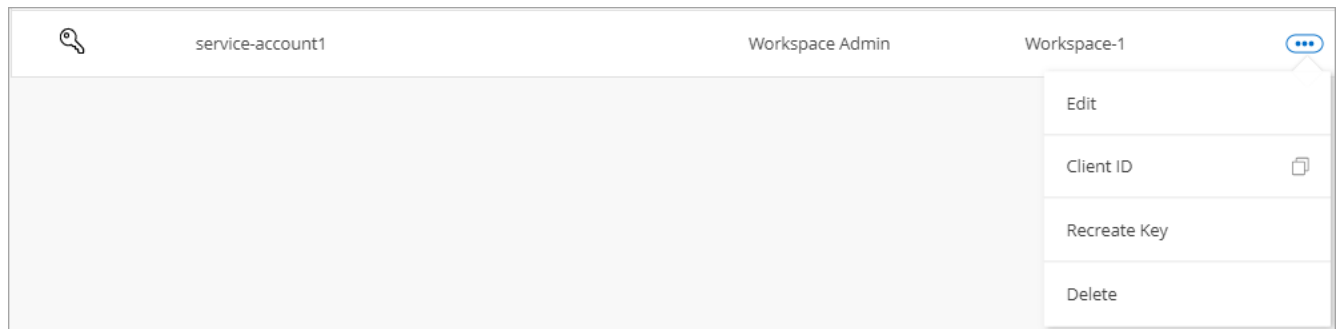
["Aprenda a crear un token de cuenta de servicio"](#)

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.



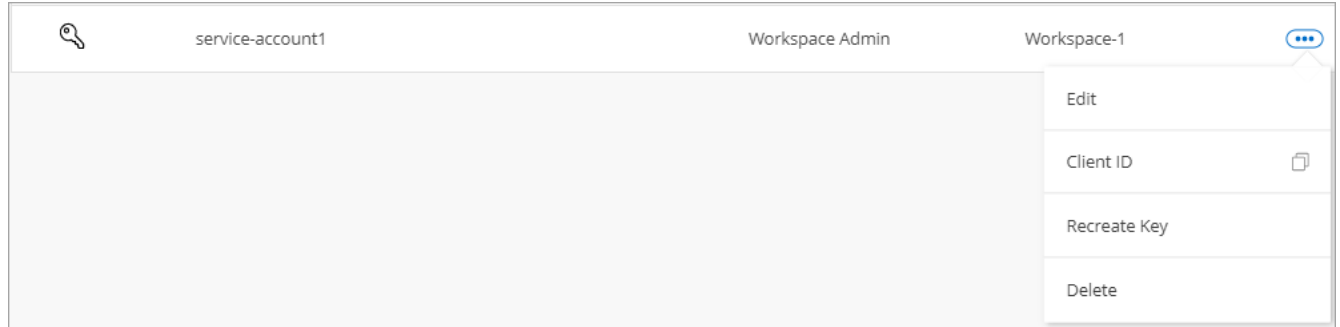
2. Haga clic en **ID de cliente**.
3. El ID se copia en el portapapeles.

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.

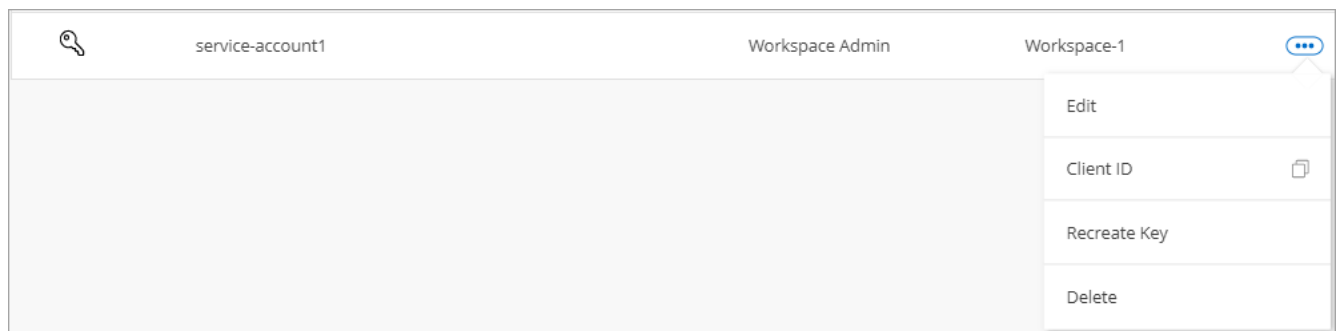
5. Haga clic en **Cerrar**.

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**.

Desactivación de la plataforma SaaS

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

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

- Backup en el cloud

Cloud Backup es compatible en regiones gubernamentales cuando la plataforma SaaS está deshabilitada, pero no en regiones comerciales cuando la plataforma SaaS está deshabilitada

- Cloud Data SENSE
- Kubernetes
- Organización en niveles del cloud
- Caché de archivos global

Si deshabilita la plataforma SaaS, deberá realizar todas las tareas desde ["La interfaz de usuario local que está disponible en un conector"](#).



Esta es una acción irreversible que le impedirá utilizar la plataforma SaaS BlueXP. Deberá realizar acciones desde el conector local. No tendrá la capacidad de usar muchos de los servicios de cloud integrados de NetApp; para volver a habilitar la plataforma SaaS será necesario contar con la ayuda de soporte 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 **Descripción general**, active la opción para desactivar el uso de la plataforma SaaS.

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

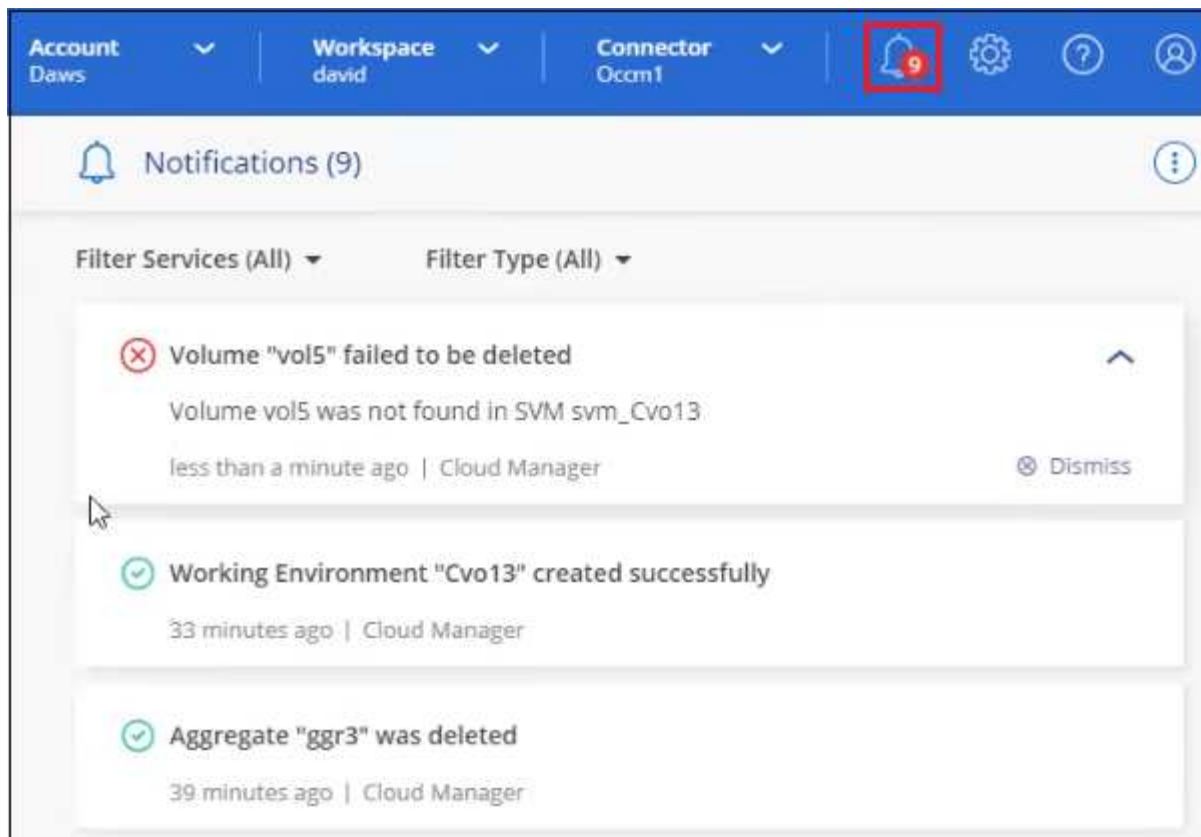
entender lo que cada uno puede ofrecer.

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.

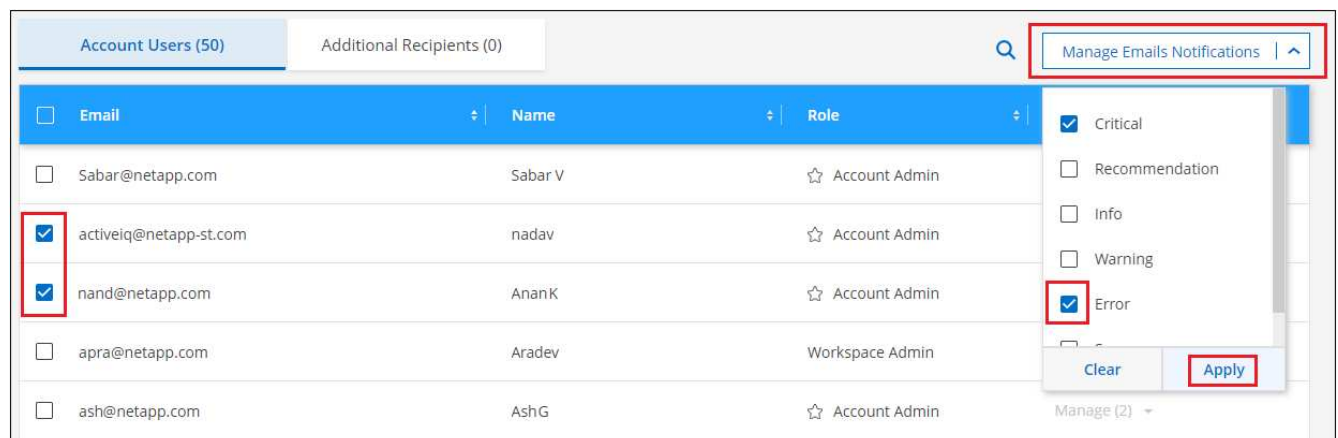
Debe ser un administrador de cuentas para personalizar los ajustes de notificaciones.

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**.



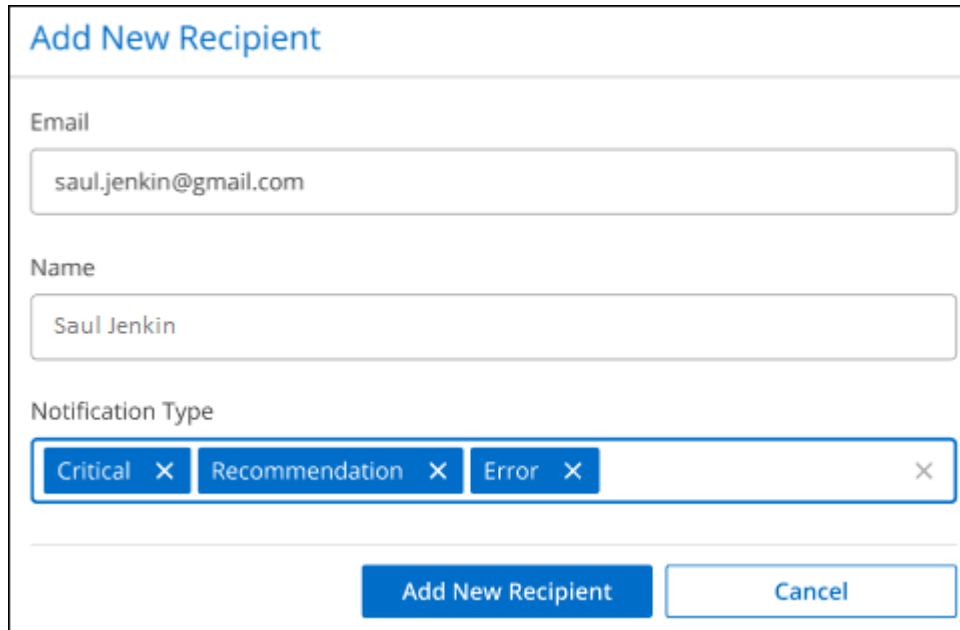
Adición de destinatarios de correo electrónico adicionales

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

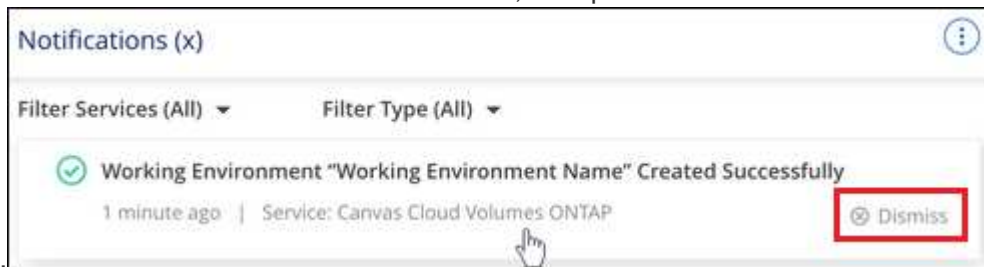
Puede eliminar notificaciones de la página si ya no necesita verlos. Puede descartar todas las notificaciones al mismo tiempo o descartar notificaciones individuales.

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.

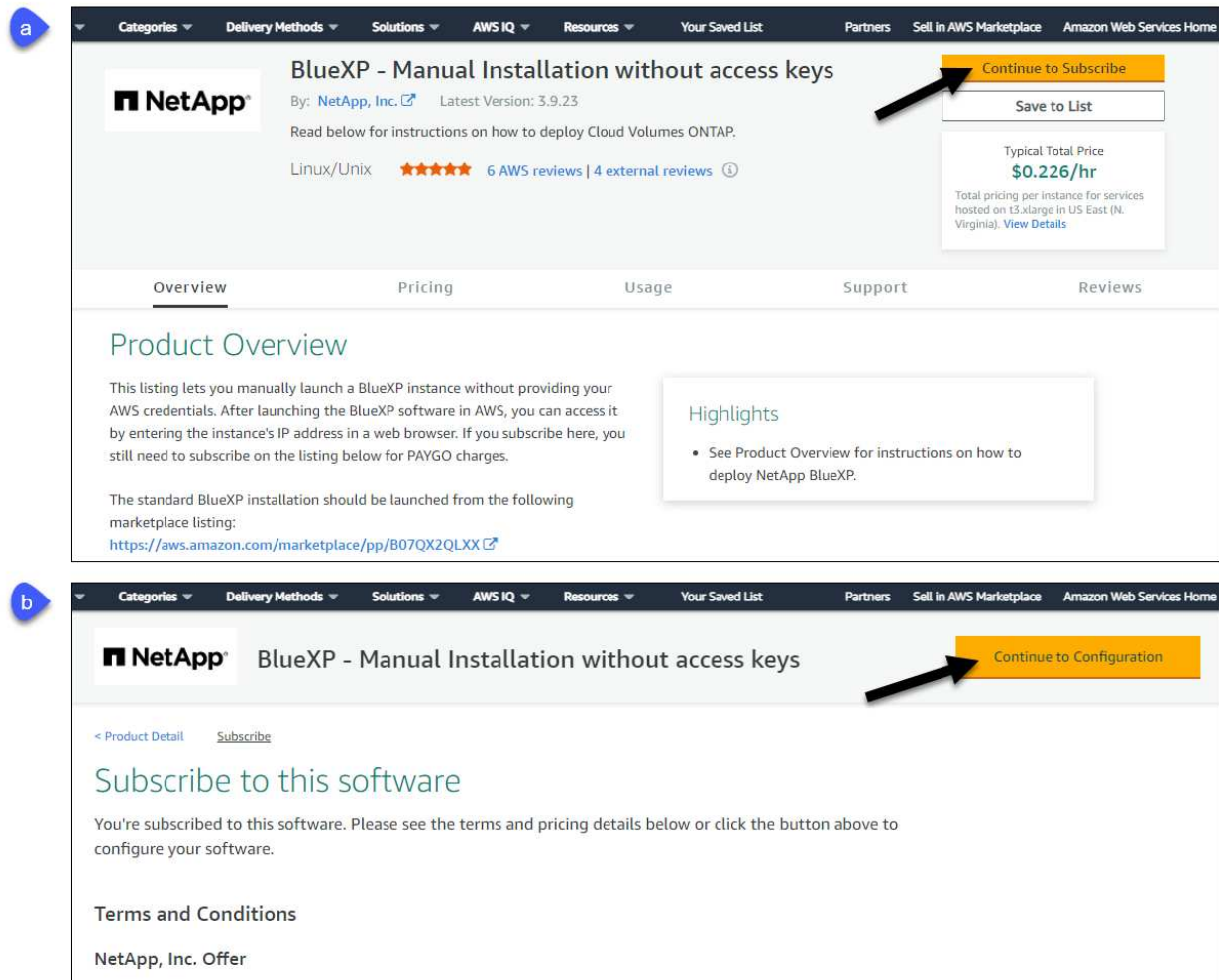
Antes de empezar

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

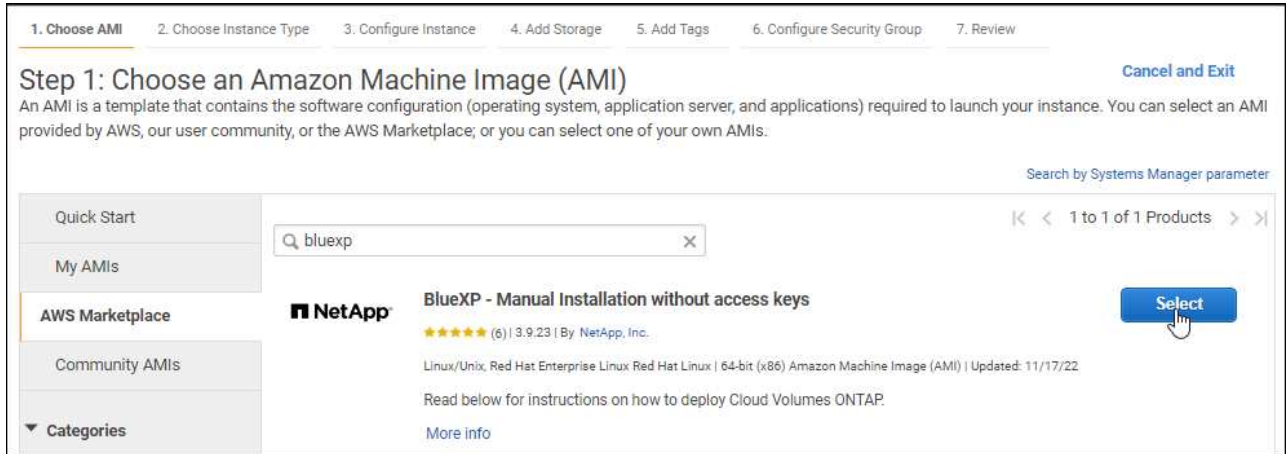
Para poner en marcha Connector en una región AWS Government, debe ir al servicio EC2 y seleccionar la oferta BlueXP en AWS Marketplace.

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	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2 VPC4QA (default)	Create new VPC
Subnet	subnet-39536c13 QASubnet1 us-east-1b 155 IP Addresses available	Create new subnet
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	Create new Capacity Reservation
IAM role	Cloud_Manager	Create new IAM role
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 Additional charges apply.	

- **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.

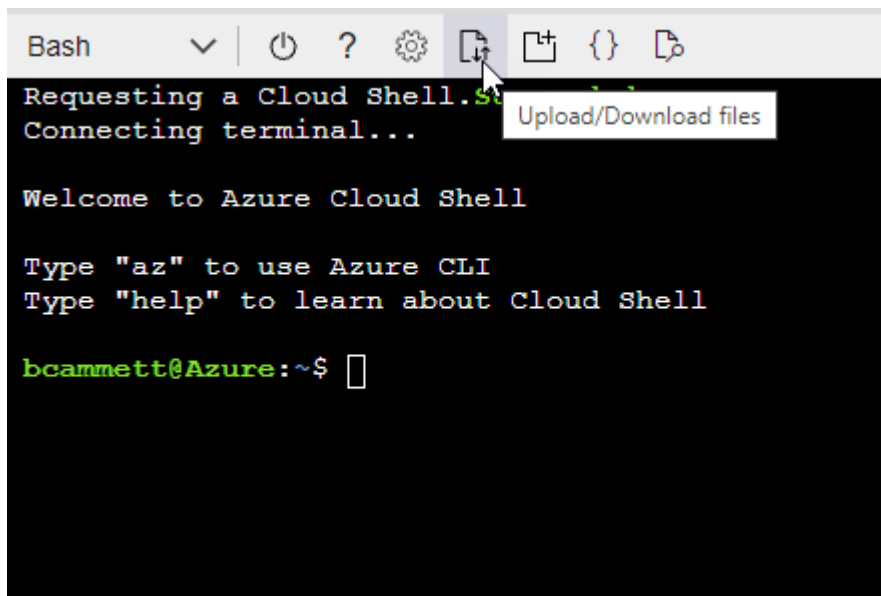
ejemplo

```
"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
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

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

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 el entorno local sin acceso a Internet

Puede instalar el conector en un host Linux local que no tenga acceso a Internet. A continuación, puede detectar clústeres de ONTAP en las instalaciones, replicar datos entre ellos, realizar backups de volúmenes mediante Cloud Backup y analizarlos con Cloud Data Sense.

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
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

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 software del conector de ["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-v3.9.23
```

5. Ejecute el script de instalación:

```
sudo /path/cloud-manager-connector-offline-v3.9.23
```

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

- ["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"

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

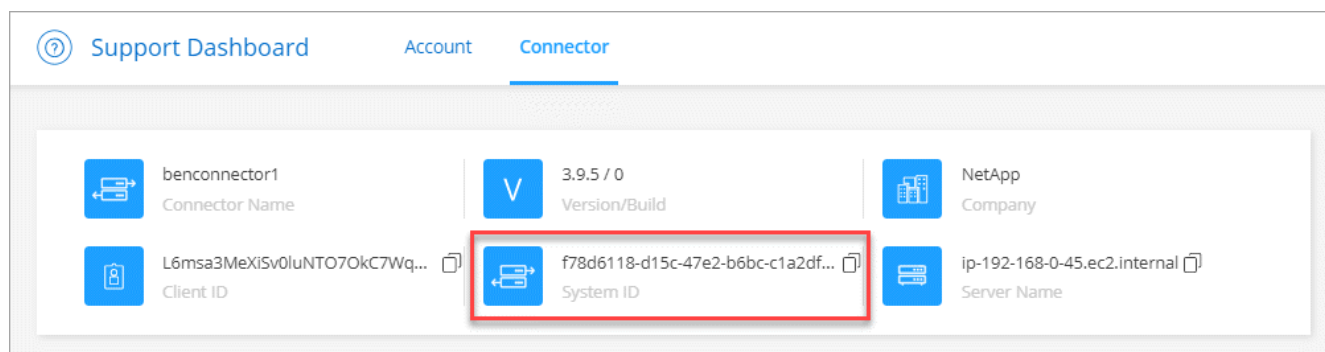
Para ayudarle a comenzar, es posible que su representante de NetApp le solicite el ID de sistema para un conector. El ID se utiliza normalmente para licencias y solución de problemas.

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

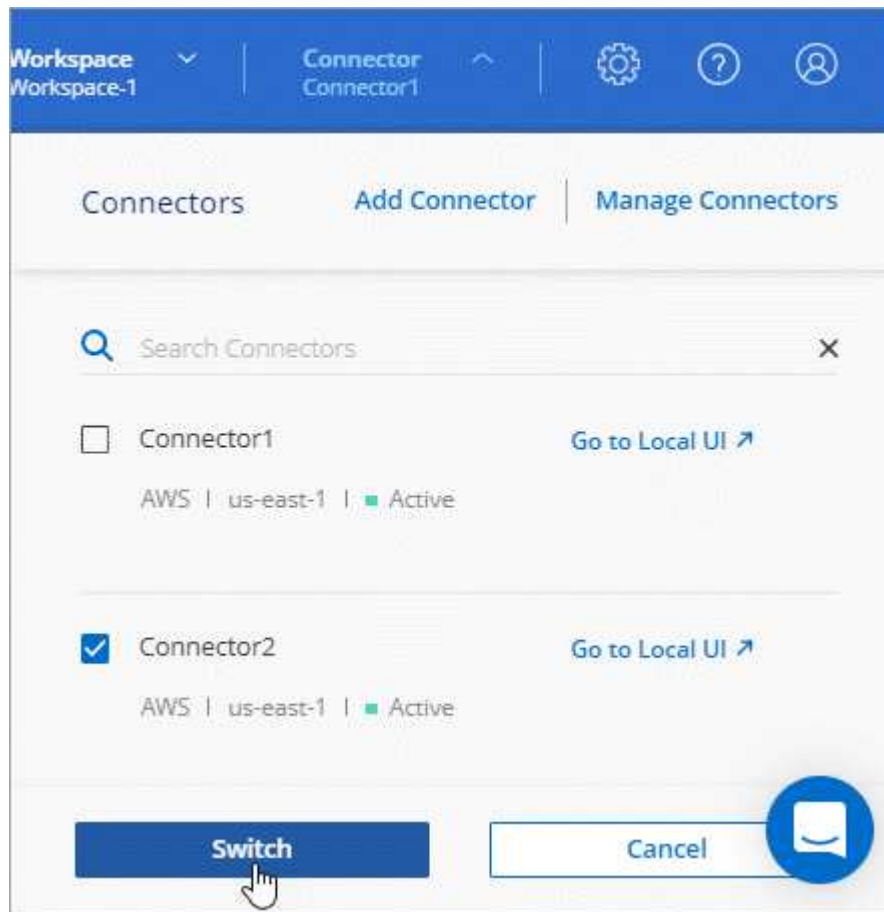
Si tiene varios conectores, puede alternar entre ellos para ver los entornos de trabajo asociados a un conector específico.

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.

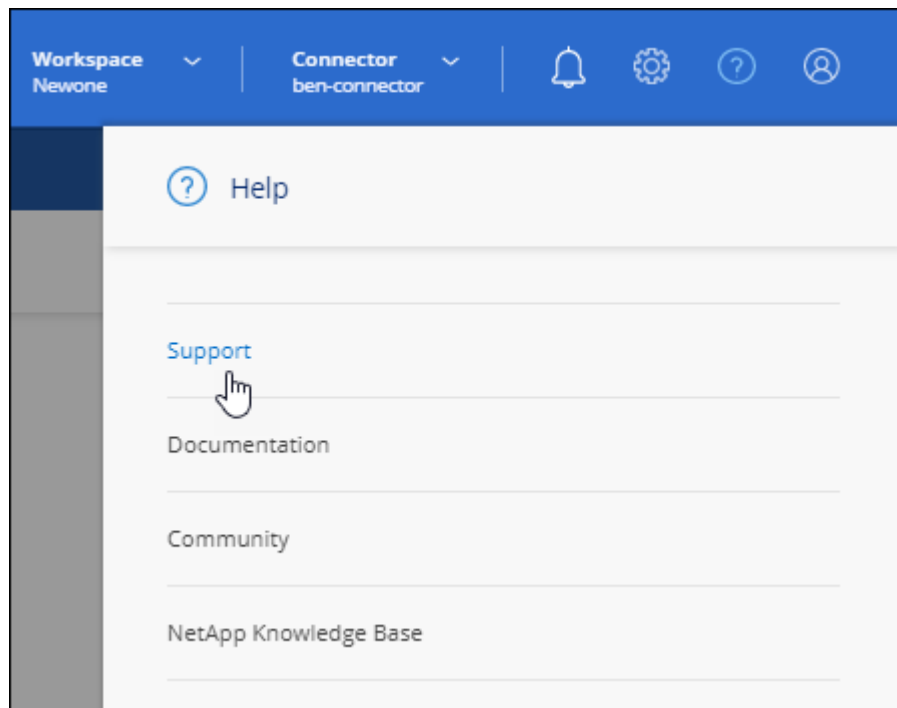
2. Introduzca su nombre de usuario y contraseña para iniciar sesión.

Descargar o enviar un mensaje de AutoSupport

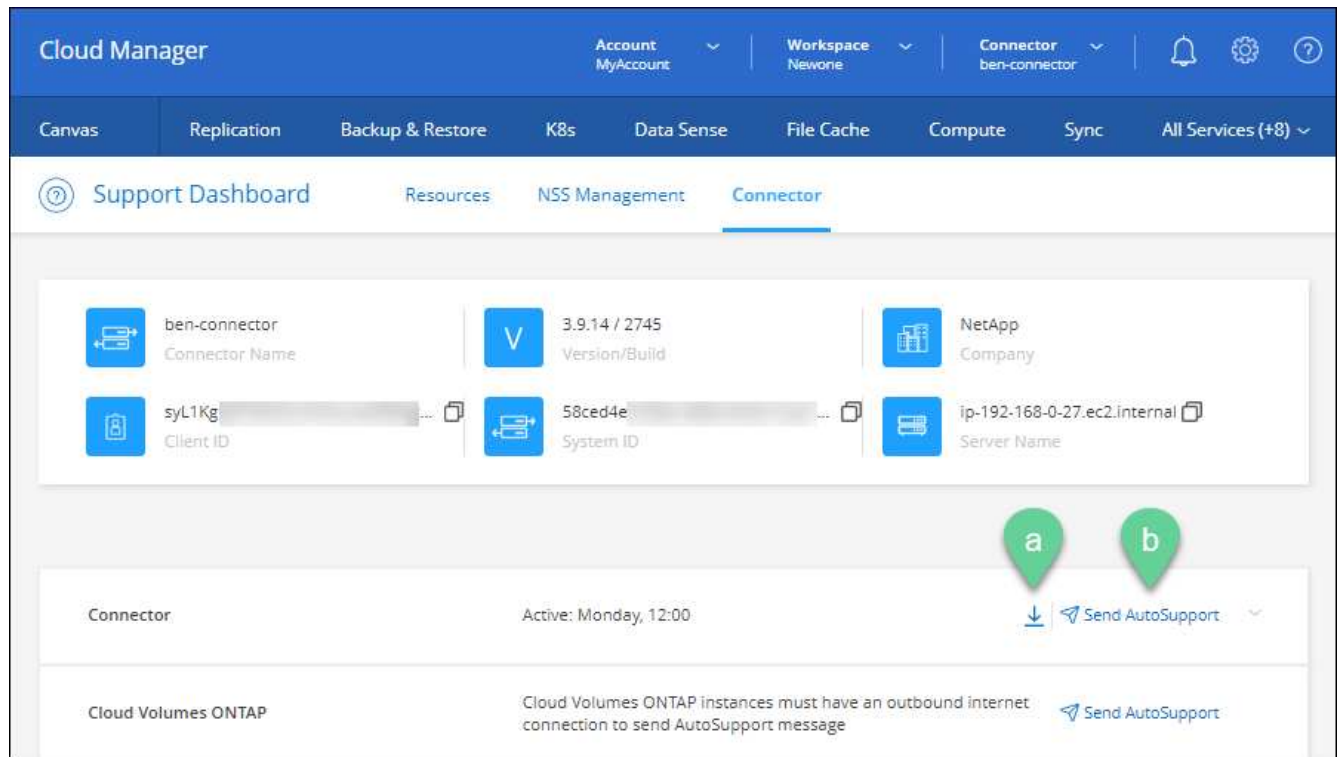
Si tiene problemas, es posible que el personal de NetApp le solicite enviar un mensaje de AutoSupport al soporte de NetApp para la solución de problemas.

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 el entorno local sin acceso a Internet

Si usted ["Se instaló el conector en un host local que no tiene 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-v3.9.14
```

4. Ejecute el script de instalación:

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

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

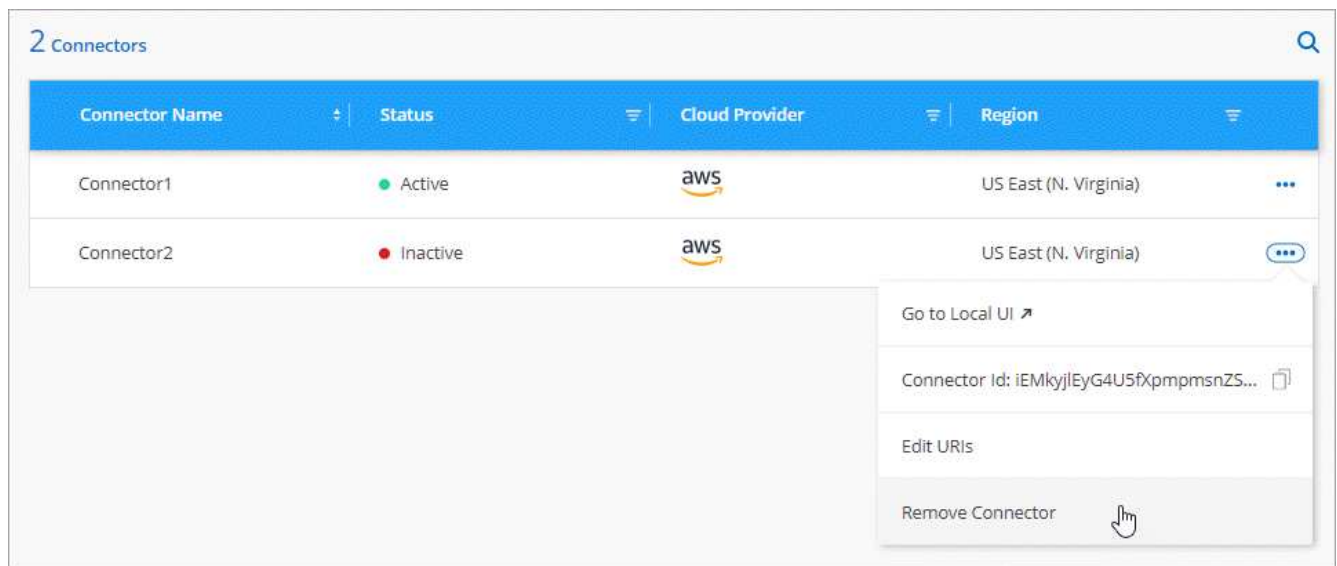
Si un conector está inactivo, puede eliminarlo de la lista de conectores de BlueXP. Puede hacerlo si ha eliminado la máquina virtual conector o si ha desinstalado el software conector.

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**.

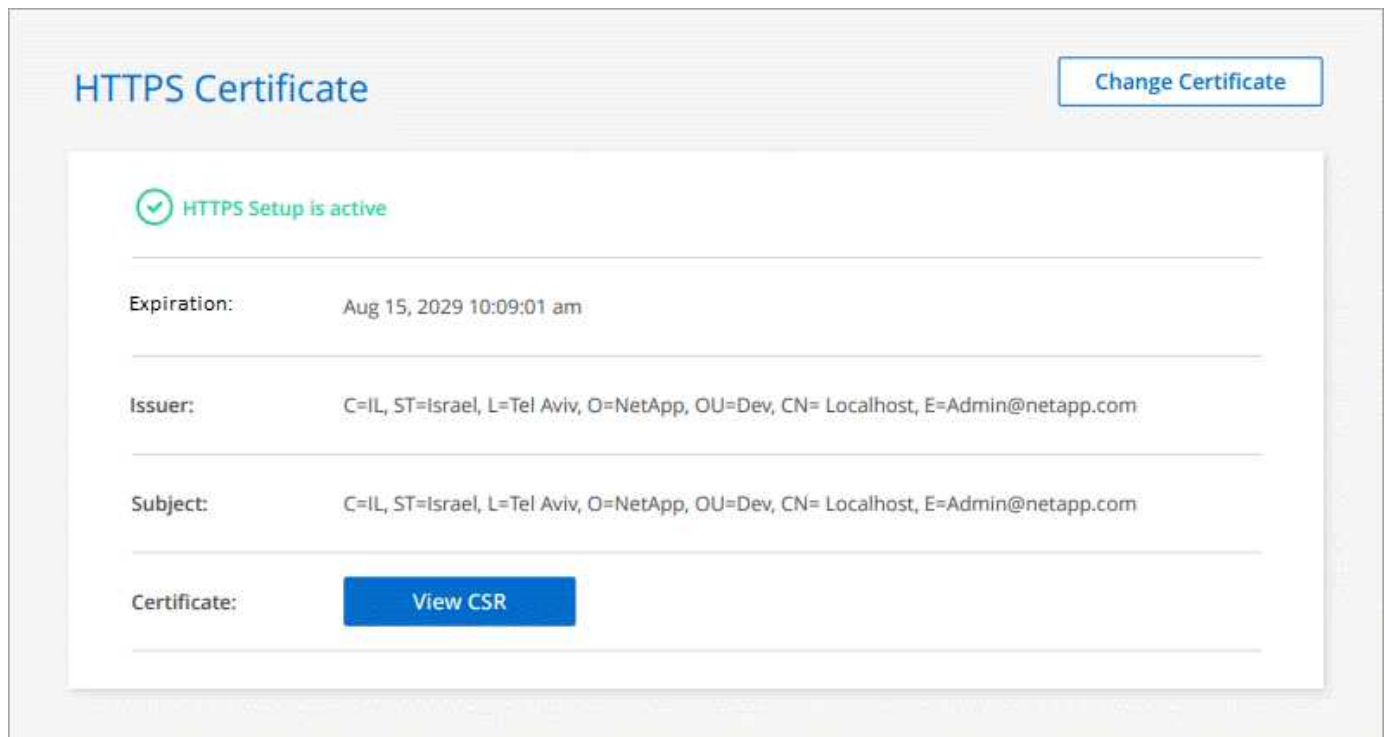


2. En la página HTTPS Setup, instale un certificado generando una solicitud de firma de certificación (CSR) o instalando su propio certificado firmado por una CA:

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 generar CSR.</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 instalar.</p>
Instale su propio certificado firmado por CA	<p>a. Seleccione instalar certificado firmado por CA.</p> <p>b. Cargue el archivo de certificado y la clave privada y, a continuación, haga clic en instalar.</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.

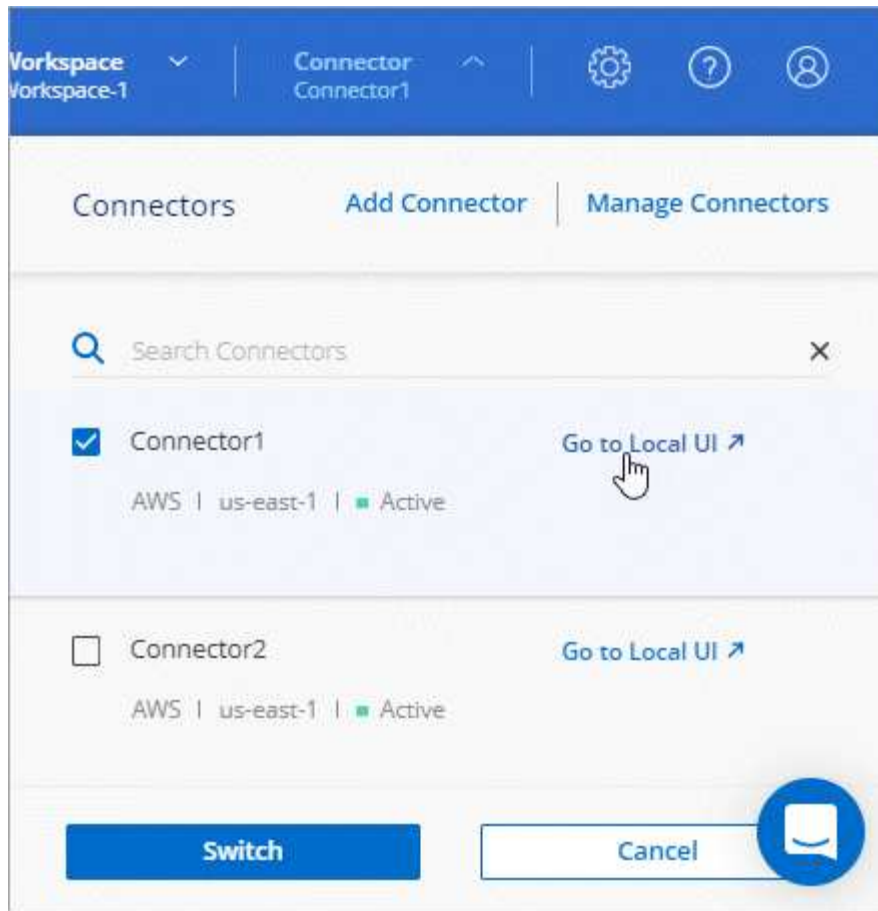
Tenga en cuenta que esta operación reinicia el conector. Asegúrese de que el conector no realiza ninguna operación antes de continuar.

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 servidor proxy, puede enviar llamadas API directamente a BlueXP sin pasar por el proxy. Esta opción es compatible con conectores que se ejecutan en AWS, en Azure o en Google Cloud.

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

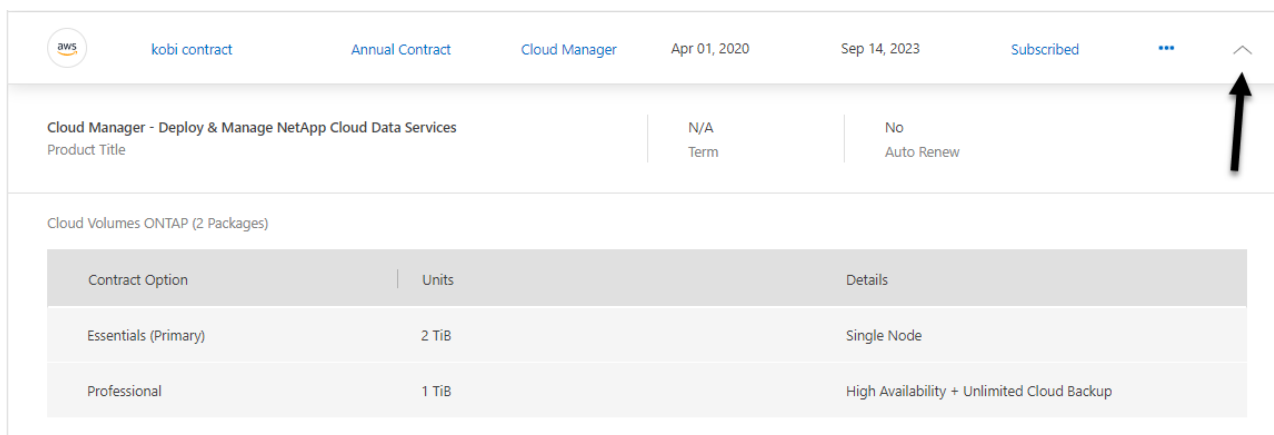
La cartera digital proporciona detalles sobre cada suscripción a PAYGO y el contrato anual asociado con su cuenta BlueXP y con Astra (Astra utiliza el servicio de carga de BlueXP).


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	aws-sub-a2	PAYGO	Cloud Manager	Apr 02, 2020	N/A	Subscribed	⋮
aws	Aleksey_aws_marketplace	Annual Contract	Astra	Oct 18, 2022	Oct 18, 2023		⋮
aws	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

Ver los 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

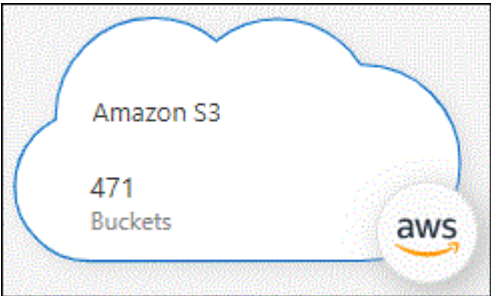
instalado el conector. Se añade un entorno de trabajo de Amazon S3 al lienzo para poder ver esta información.

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.


Pasos

- 1. "Instale un conector" En la cuenta de AWS, donde desea ver sus bloques de Amazon S3.
- 2. En el menú de navegación, selecciona **almacenamiento > Canvas**.

Verá automáticamente un entorno de trabajo de Amazon S3 poco después.



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



Amazon S3

■


 On

471

Buckets

INFORMATION

SERVICES




Sync


■

 On

35.48 TiB

Data Synced






Data Sense

■

 Off

Enable



Enter Working Environment

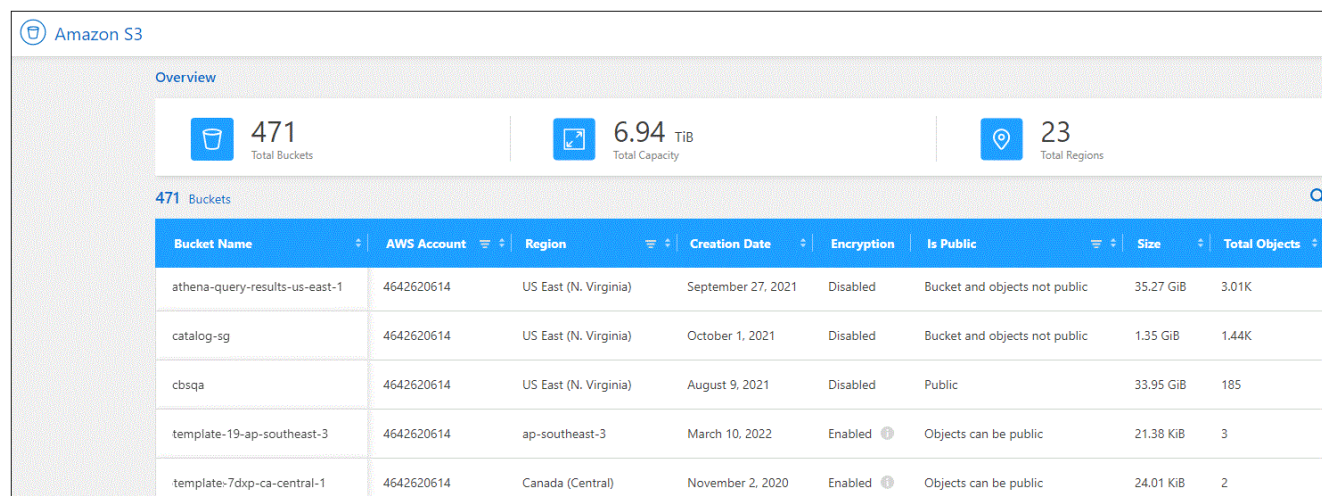
4. Haga clic en **Sincronizar datos** para sincronizar datos con o desde bloques S3.

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

5. Haga clic en **Activar** si desea que Cloud Data Sense analice los cubos de S3 en busca de datos personales y confidenciales.

Para obtener información detallada, consulte ["Introducción a Cloud Data Sense para Amazon S3"](#).

6. Haga clic en **Entrar en entorno de trabajo** para ver detalles sobre los bloques S3 de su cuenta de AWS.



The screenshot shows the Amazon S3 Overview page. At the top, there are three summary cards: '471 Total Buckets', '6.94 TiB Total Capacity', and '23 Total Regions'. Below these is a table titled '471 Buckets' with the following columns: Bucket Name, AWS Account, Region, Creation Date, Encryption, Is Public, Size, and Total Objects. The table lists five buckets with their respective details.

Bucket Name	AWS Account	Region	Creation Date	Encryption	Is Public	Size	Total Objects
athena-query-results-us-east-1	4642620614	US East (N. Virginia)	September 27, 2021	Disabled	Bucket and objects not public	35.27 GiB	3.01K
catalog-sg	4642620614	US East (N. Virginia)	October 1, 2021	Disabled	Bucket and objects not public	1.35 GiB	1.44K
cbsqa	4642620614	US East (N. Virginia)	August 9, 2021	Disabled	Public	33.95 GiB	185
template-19-ap-southeast-3	4642620614	ap-southeast-3	March 10, 2022	Enabled	Objects can be public	21.38 KiB	3
template-7dxc-ca-central-1	4642620614	Canada (Central)	November 2, 2020	Enabled	Objects can be public	24.01 KiB	2

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.

 **Azure Blob Storage** 



 On

INFORMATION


55

Storage Accounts

SERVICES

 **Sync**
 On

20 MiB
Data Synced




[Enter Working Environment](#)


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
ovu8llxvdfypxn	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
bu9kixthymr1be	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	1.01 MiB
8jzsvybvjwieww8	OCCM QA1	Canada Central	December 12, 2019	aff1-rg	170 B

Visualización de sus buckets de Google Cloud Storage

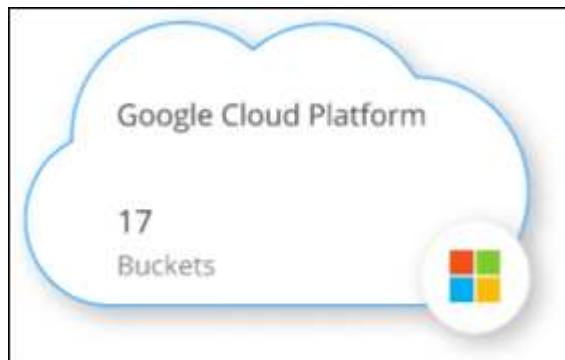
Después de instalar un conector en Google Cloud, BlueXP puede descubrir automáticamente información sobre los cubos de Google Cloud Storage que residen en la cuenta de Google donde está instalado el conector. Se añade un entorno de trabajo de Google Cloud Storage al lienzo para que puedas ver esta información.

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.

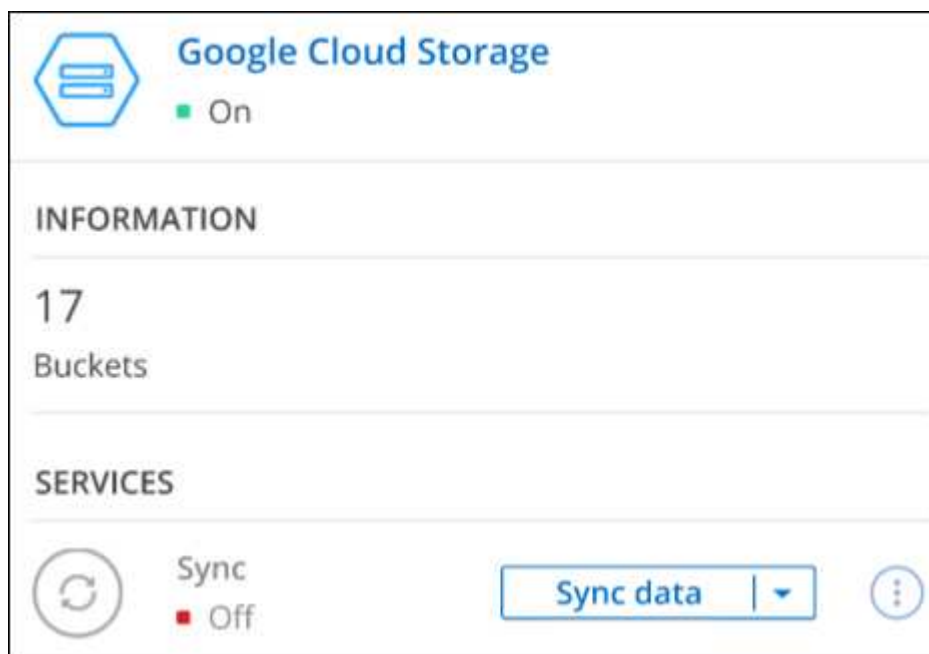
Pasos

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.



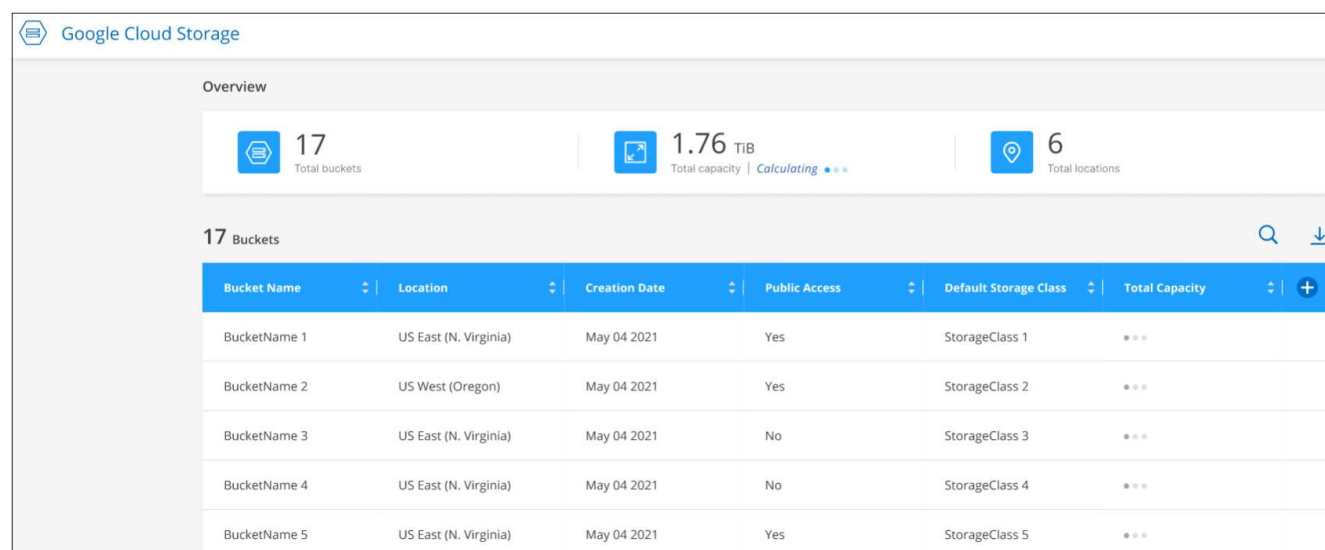
3. Haga clic en el entorno de trabajo y seleccione una acción en el panel derecho.



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

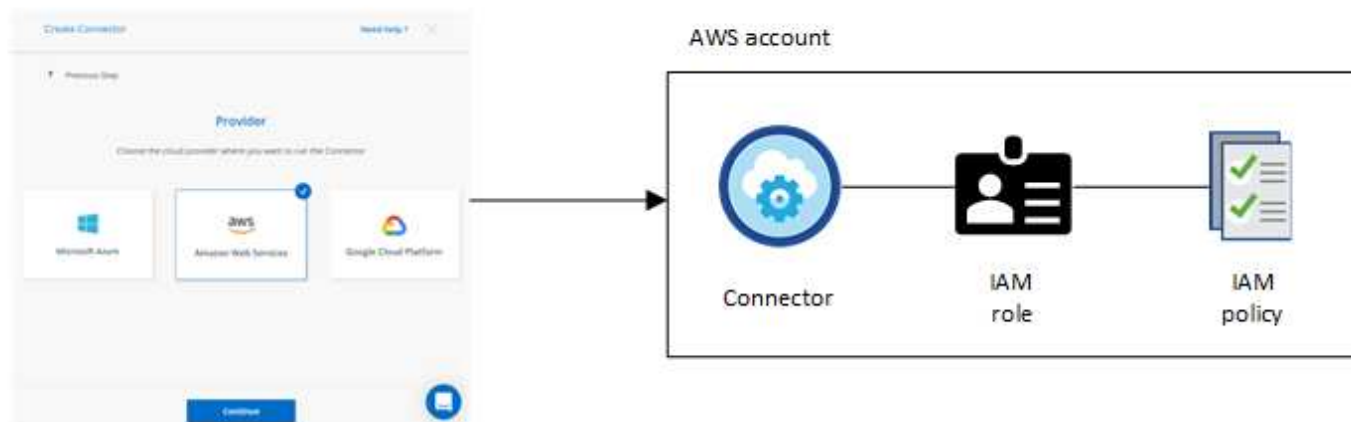
Credenciales y permisos de AWS

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:

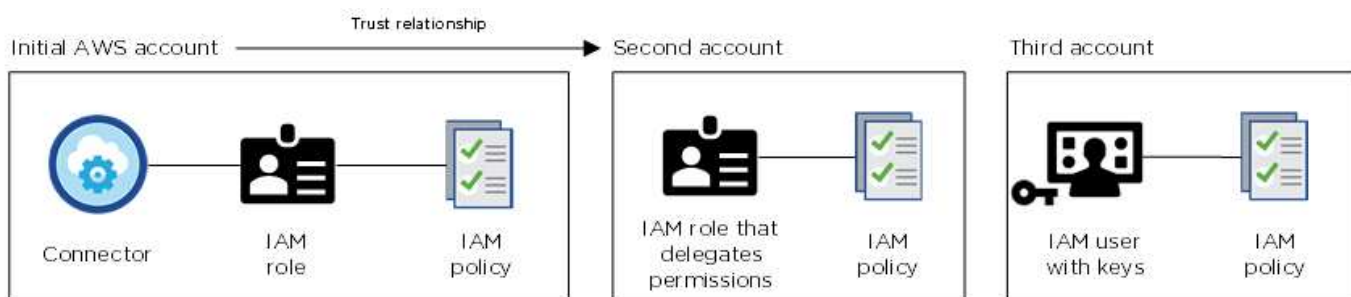
Details & Credentials			
Instance Profile Credentials	Account ID	QA Subscription Marketplace Subscription	Edit Credentials

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: [redacted]

Instance Profile | Account ID: [redacted]

● 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: [redacted]
- Instance Profile | Account ID: [redacted]
- 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 (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

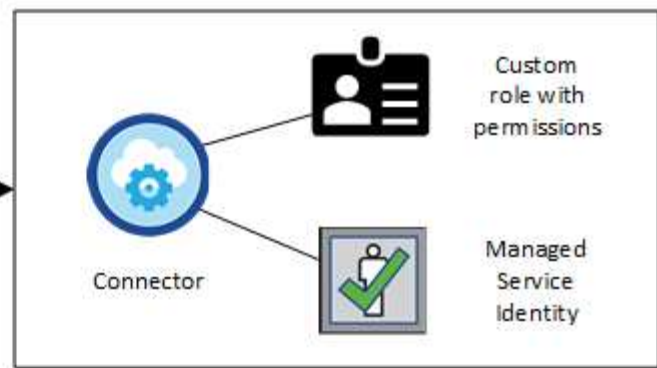
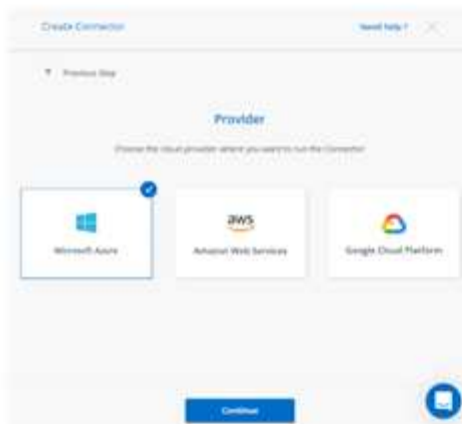
Credenciales y permisos de Azure

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	ⓘ No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

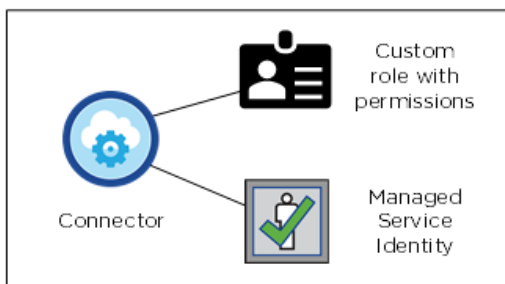
Suscripciones adicionales de Azure para una identidad gestionada

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"](#).

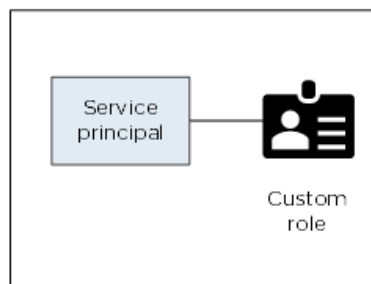
Credenciales adicionales de Azure

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:

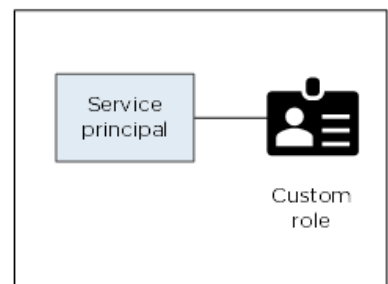
Initial Azure account



Second account



Third account

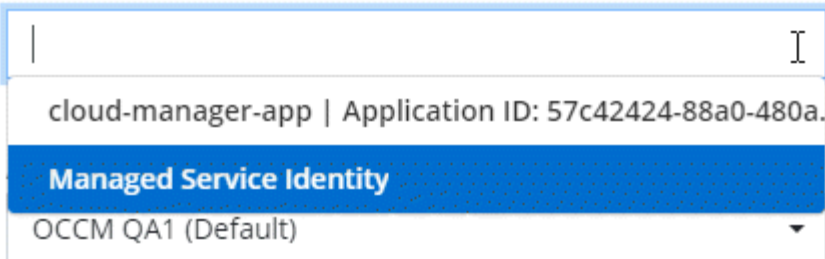


Entonces lo haría ["Agregue las credenciales de cuenta a BlueXP"](#) Proporcionando detalles acerca del director de servicio de AD.

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

Edit Account & Add Subscription

Credentials



cloud-manager-app | Application ID: 57c42424-88a0-480a.

Managed Service Identity

OCCM QA1 (Default)

¿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.

Gestión de 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

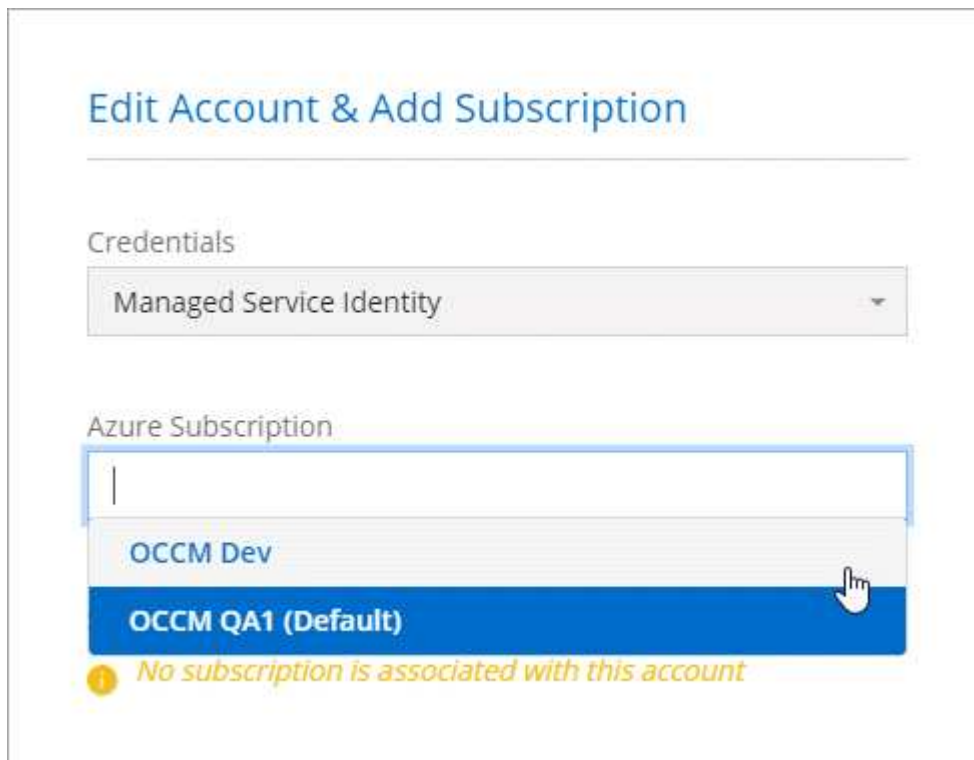
1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar Cloud Volumes ONTAP.
3. Haga clic en **Control de acceso (IAM)**.
 - a. Haga clic en **Agregar > Agregar asignación de rol** y, a continuación, agregue los permisos:
 - Seleccione el rol **operador de BlueXP**.
 - Asigne acceso a una **máquina virtual**.
 - Seleccione la suscripción en la que se creó la máquina virtual Connector.
 - Seleccione la máquina virtual conector.
 - Haga clic en **Guardar**.
4. Repita estos pasos para suscripciones adicionales.



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

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"](#).

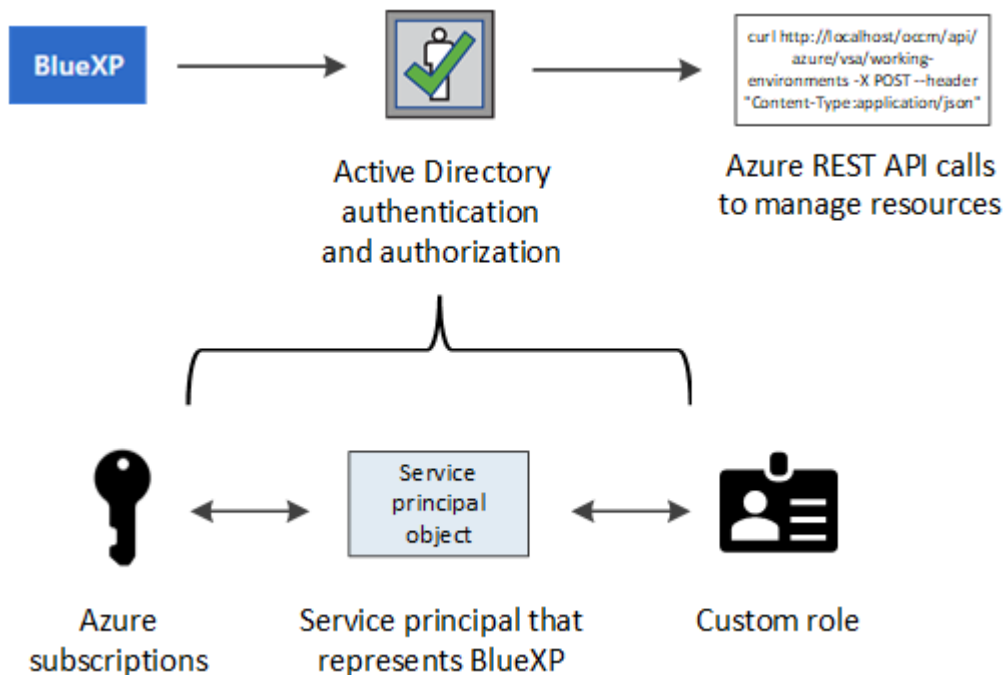
Si desea implementar Cloud Volumes ONTAP con credenciales de *diferente* Azure, debe conceder los permisos necesarios para crear y configurar un director de servicio en Azure Active Directory para cada cuenta de Azure. A continuación, puede agregar las nuevas credenciales a BlueXP.

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

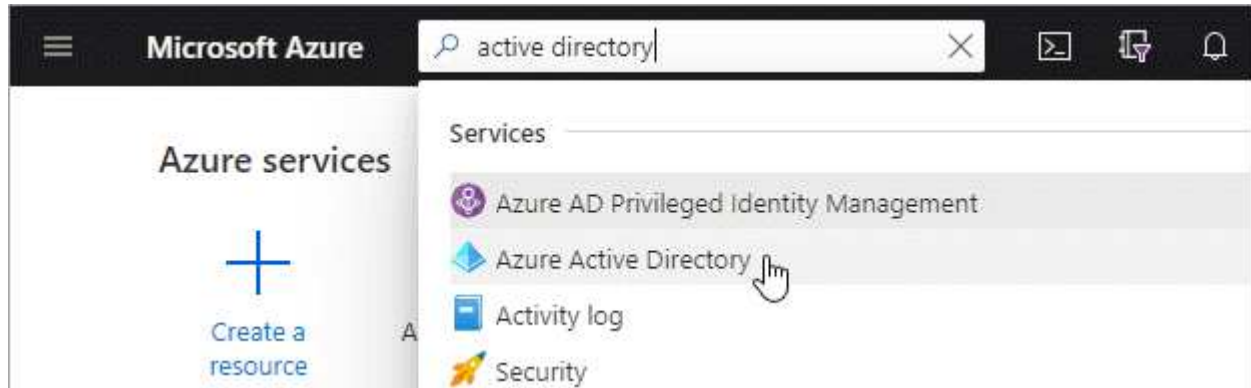
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que BlueXP pueda usar para el control de acceso basado en roles.

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.

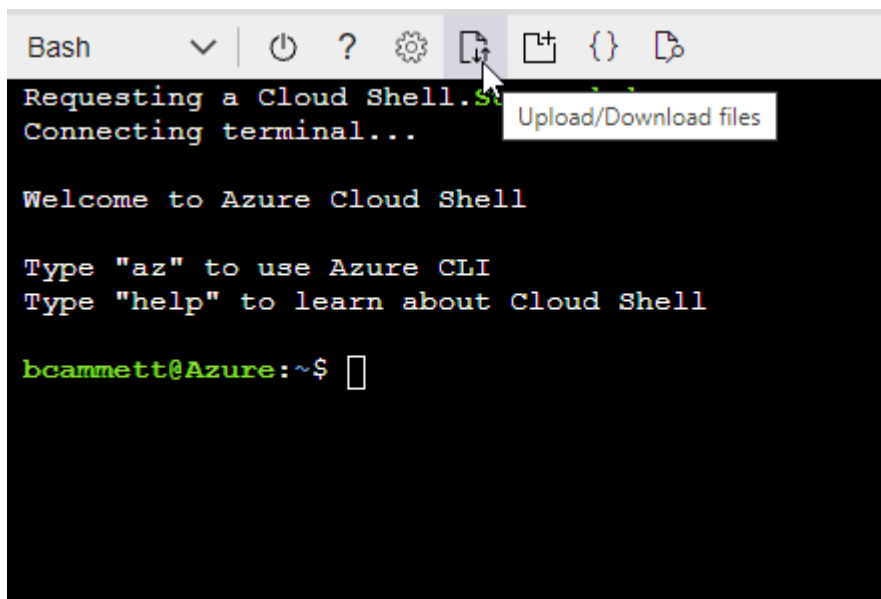
ejemplo

```
"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:

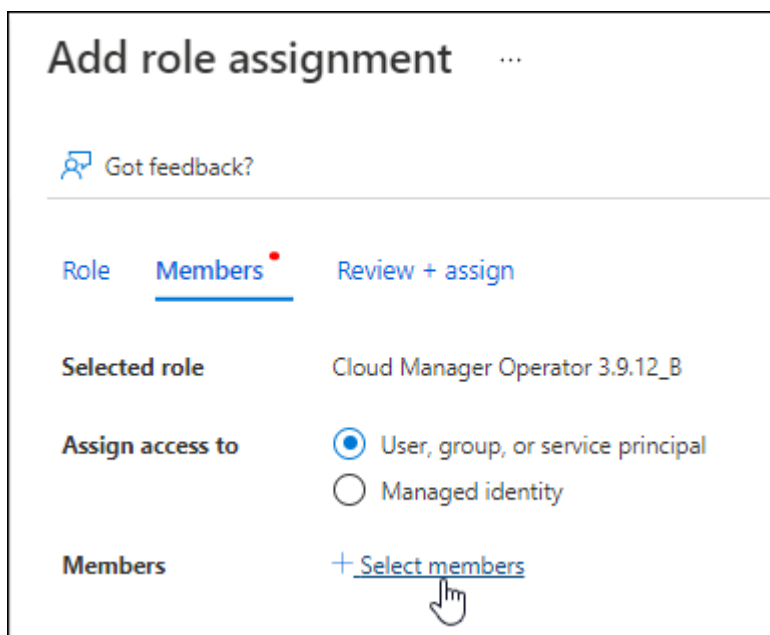
```
az role definition create --role-definition Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

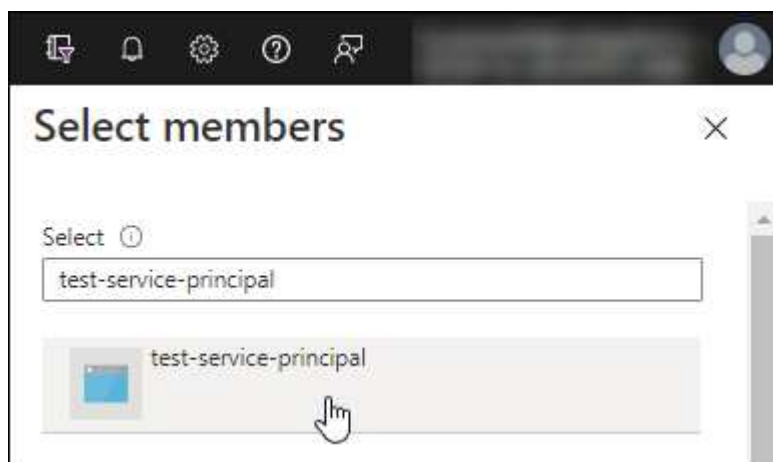
- a. En el portal de Azure, abra el servicio **Suscripciones**.
- b. Seleccione la suscripción.
- c. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
- d. En la ficha **rol**, seleccione el rol **operador BlueXP** y haga clic en **Siguiente**.
- e. En la ficha **Miembros**, 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.

 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 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"/> user_impersonation 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**.



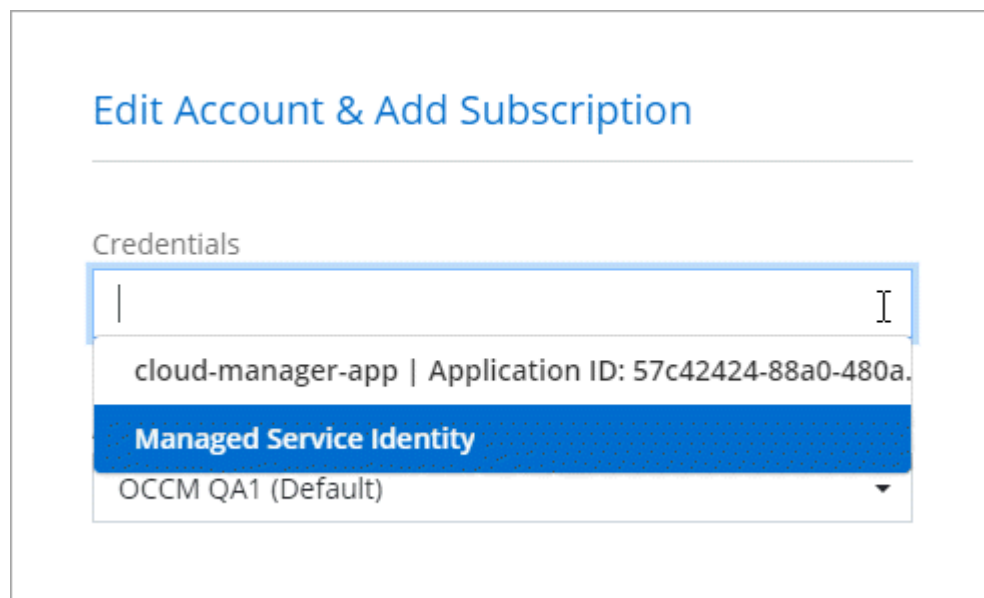
- Haga clic en **Agregar credenciales** y siga los pasos del asistente.
 - Ubicación de credenciales:** Seleccione **Microsoft Azure > conector**.
 - Definir credenciales:** Introduzca información acerca del principal de servicio de Azure Active Directory que otorga los permisos necesarios:
 - ID de 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:

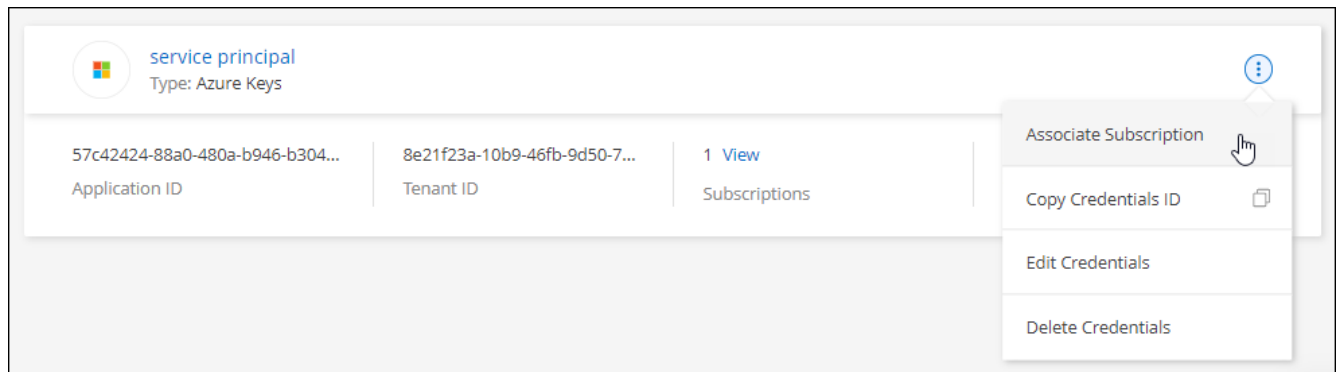
- No asoció una suscripción cuando agregó inicialmente las credenciales a BlueXP.
- Desea sustituir una suscripción existente de Azure Marketplace por una nueva suscripción.

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

(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

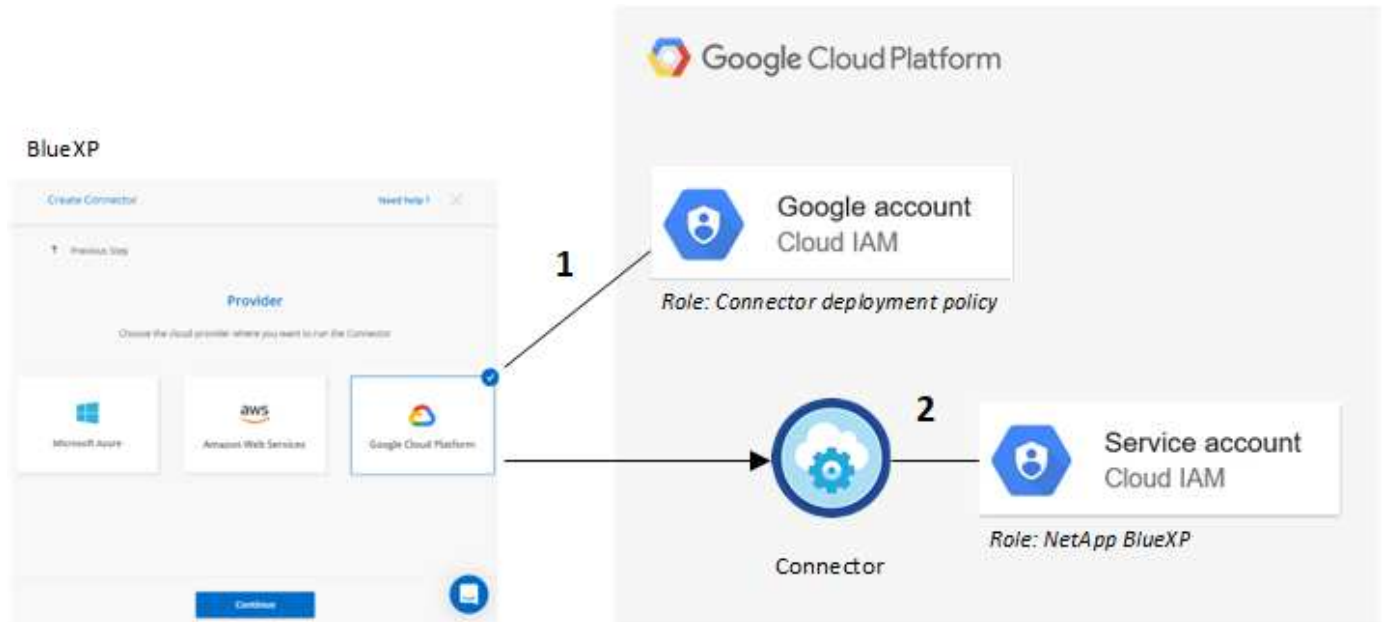
Antes de poder poner en marcha Cloud Volumes ONTAP en Google Cloud, primero debe poner en marcha un conector en un proyecto de Google Cloud. El conector no puede ejecutarse en sus instalaciones ni en un proveedor de cloud diferente.

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.

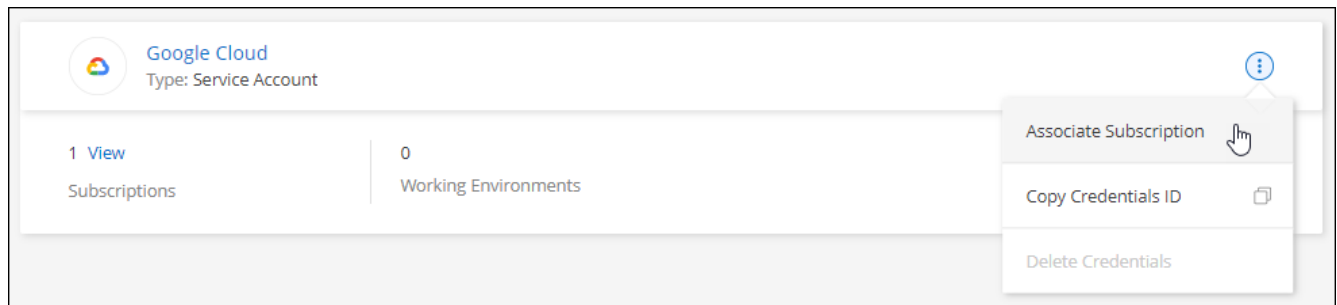
Asociación de una suscripción a Marketplace con credenciales de Google Cloud

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.

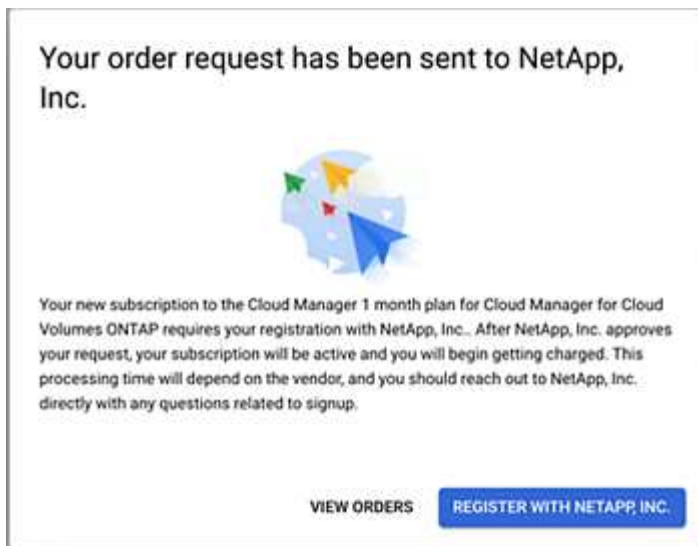
The screenshot shows the 'Product details' page for NetApp BlueXP on the Google Cloud platform. At the top, there's a navigation bar with the Google Cloud logo and a dropdown menu showing 'netapp.com'. Below this, a back arrow and the text 'Product details' are visible. The main content area features 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.' Below this is a prominent blue 'SUBSCRIBE' button. A horizontal menu contains links for 'OVERVIEW', 'PRICING', 'DOCUMENTATION', and 'SUPPORT', with 'OVERVIEW' being the active tab. The 'Overview' section contains two paragraphs: the first describes BlueXP as a hybrid multicloud storage and data services experience, and the second explains how it abstracts Google Cloud infrastructure complexity. To the right, under 'Additional details', it lists the product type as 'SaaS & APIs', the last update date as '12/19/22', and categories as 'Analytics', 'Developer tools', and '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	⋮

Añadir y gestionar 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

Es necesario añadir una cuenta del sitio de soporte de NetApp a BlueXP para realizar las siguientes tareas:

- Para registrarse y recibir soporte
- Para poner en marcha Cloud Volumes ONTAP cuando 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.

- Para registrar 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.

- Para actualizar el software Cloud Volumes ONTAP a la versión más reciente

También tendrá que introducir sus credenciales de NSS para utilizar el asesor digital (anteriormente Active IQ) desde BlueXP. Estas credenciales se asocian directamente con su cuenta de usuario y se utilizan únicamente con el asesor digital. Revise más detalles en la siguiente sección.

Gestione una cuenta de NSS asociada con Digital Advisor

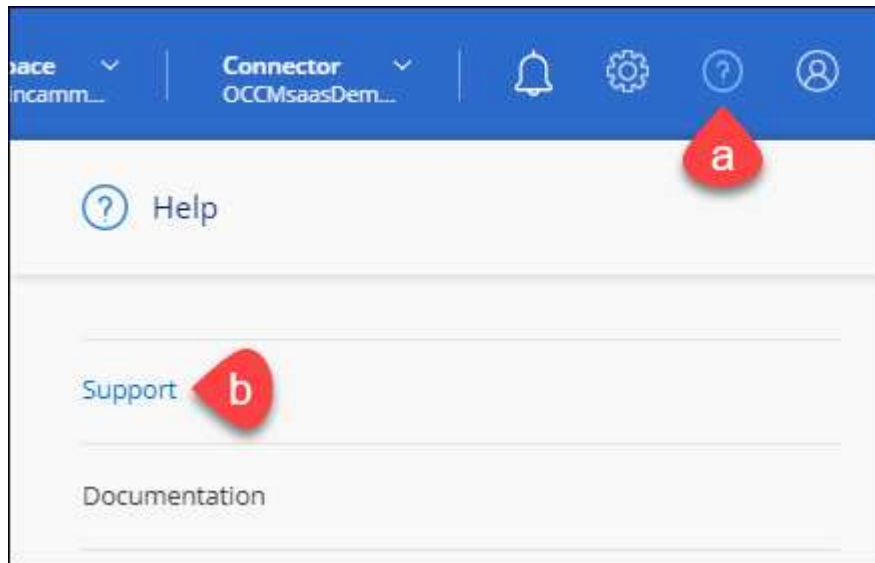
Al acceder a Digital Advisor en BlueXP, se le pedirá que inicie sesión en Digital Advisor introduciendo sus credenciales de NSS. Después de introducir sus credenciales de NSS, verá esta cuenta de NSS que aparece en la parte superior de la página NSS Management. A continuación, puede gestionar esas credenciales según sea necesario.

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, licencia o soporte de Cloud Volumes ONTAP.
- Sólo puede haber una cuenta NSS asociada con Digital Advisor, 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:** Añada credenciales para una cuenta del sitio de soporte de NetApp de manera que pueda acceder a Digital Advisor en BlueXP.
- **Actualizar las credenciales existentes:** Actualizar las credenciales de su cuenta del sitio de soporte de NetApp.
- **Eliminar:** Elimina la cuenta asociada con Digital Advisor.

Resultado

BlueXP actualiza la cuenta NSS asociada con Digital Advisor.

Añada una cuenta de NSS

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

- Si tiene una cuenta de nivel de cliente, puede añadir una o varias cuentas de NSS.
- Si tiene una cuenta de socio o distribuidor, puede agregar una o más cuentas de NSS, pero no se pueden agregar junto con 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 debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal).
- 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.

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.

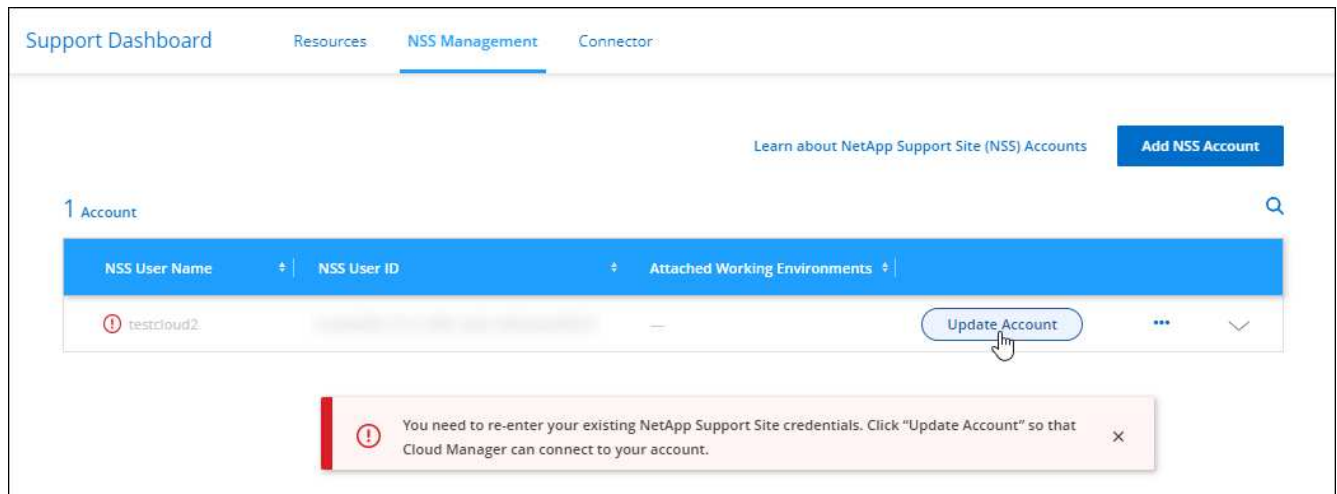
- "Inicio de Cloud Volumes ONTAP en AWS"
- "Inicio de Cloud Volumes ONTAP en Azure"
- "Lanzamiento de Cloud Volumes ONTAP en GCP"
- "Registro de sistemas de pago por uso"

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**.

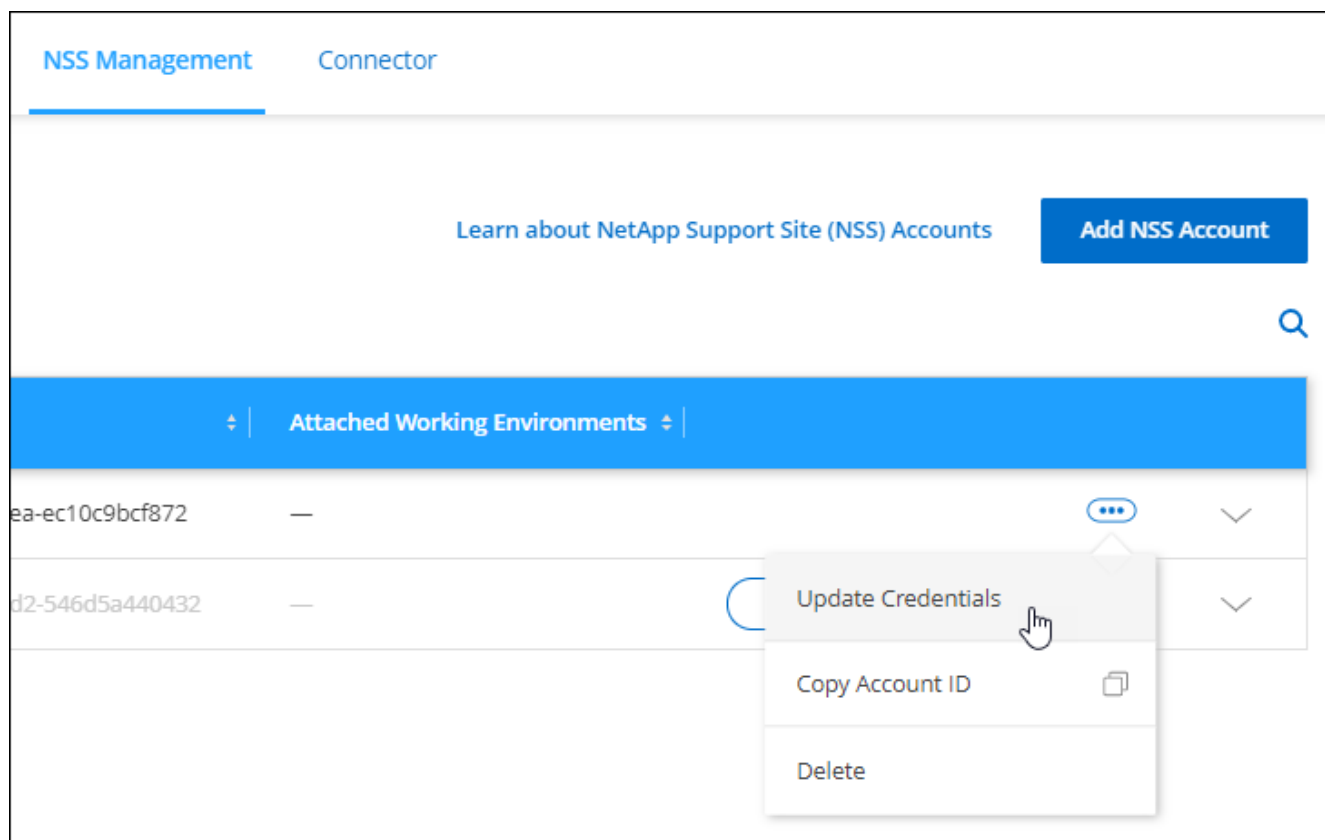
Actualice las credenciales de NSS

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.

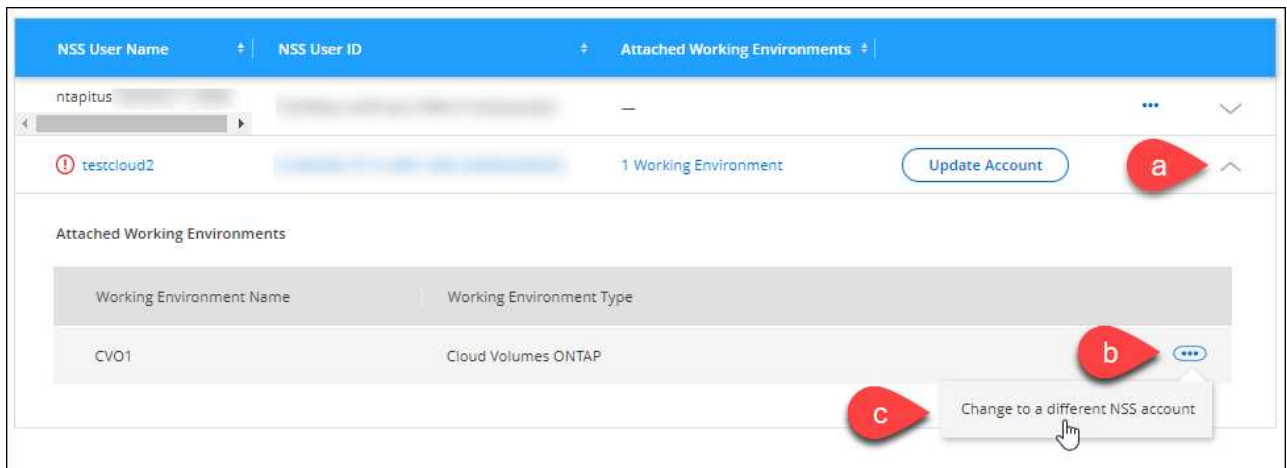
Adjunte un entorno de trabajo a una cuenta de NSS diferente

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.

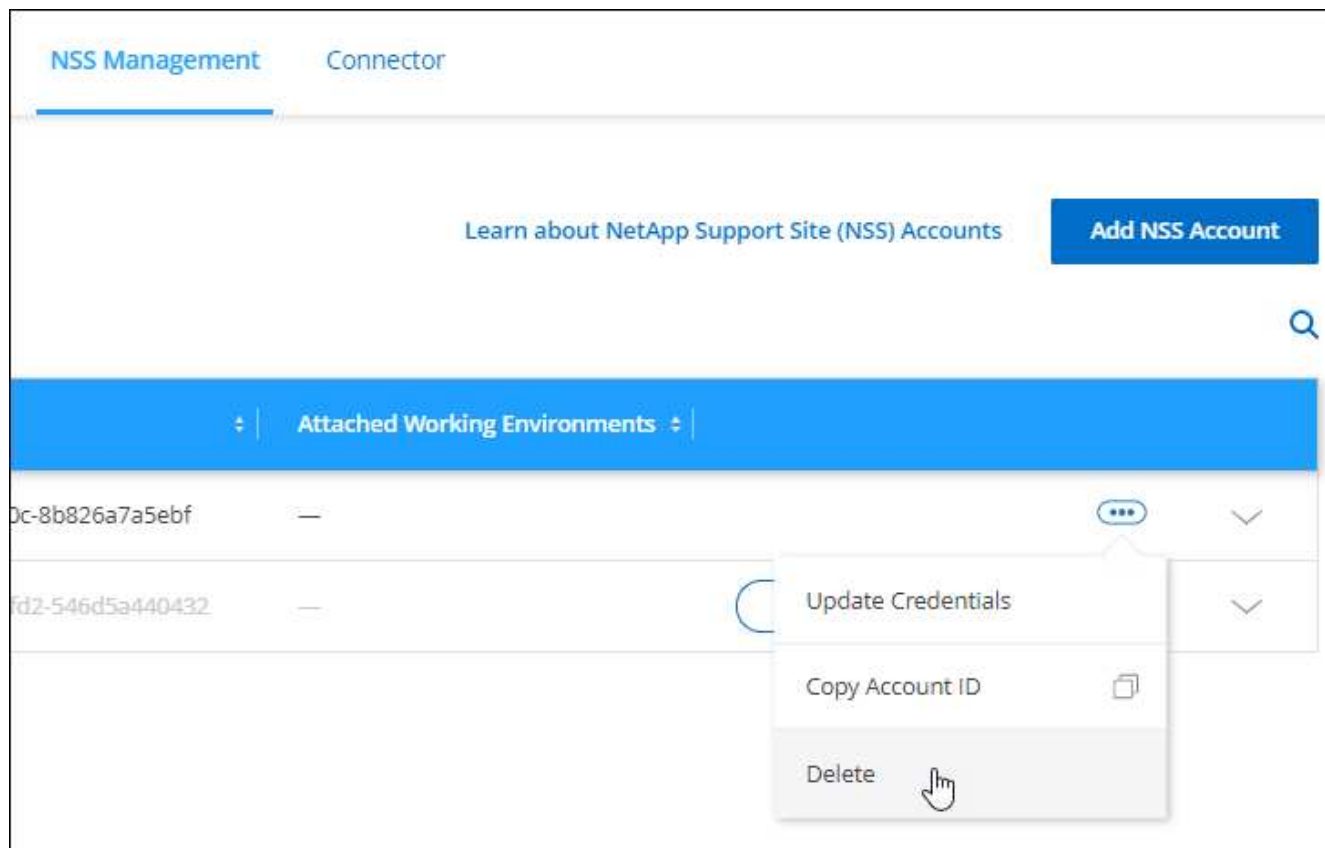
Quite una cuenta de NSS

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"](#)

Referencia

Permisos

Resumen de permisos para BlueXP

Para poder utilizar las funciones y servicios de BlueXP, deberá proporcionar permisos para que BlueXP pueda realizar operaciones en su entorno de nube. Utilice los vínculos de esta página para acceder rápidamente a los permisos que necesita en función de su objetivo.

Permisos de AWS

Específico	Descripción	Enlace
Despliegue del conector	El usuario que crea un conector a partir de BlueXP necesita permisos específicos para implementar la instancia en AWS.	"Cree un conector en AWS desde BlueXP"
Funcionamiento del conector	Cuando BlueXP inicia el conector, adjunta una directiva a la instancia que proporciona los permisos necesarios para administrar los recursos y procesos de su cuenta de AWS. Usted debe establecer la política usted mismo si usted "Inicie un conector desde el mercado" o si usted "Agregue más credenciales de AWS a un conector" . También debe asegurarse de que la directiva esté actualizada a medida que se añadan nuevos permisos en versiones posteriores.	"Permisos de AWS para Connector"
Funcionamiento de Cloud Volumes ONTAP	Se debe conectar un rol de IAM a cada nodo Cloud Volumes ONTAP en AWS. Lo mismo sucede con el mediador de alta disponibilidad. La opción predeterminada es dejar que BlueXP cree las funciones IAM para usted, pero puede utilizar las suyas propias.	"Aprenda a configurar las funciones del IAM usted mismo"

Permisos de Azure

Específico	Descripción	Enlace
Despliegue del conector	Al implementar un conector desde BlueXP, necesita utilizar una cuenta de Azure o una entidad de servicio con permisos para implementar Connector VM en Azure.	"Cree un conector en Azure desde BlueXP"

Específico	Descripción	Enlace
Funcionamiento del conector	<p>Cuando BlueXP implementa Connector VM en Azure, crea una función personalizada que proporciona los permisos necesarios para gestionar los recursos y procesos dentro de esa suscripción a Azure.</p> <p>Debe configurar la función personalizada si lo desea "Inicie un conector desde el mercado" o si usted "Agregue más credenciales de Azure a un conector".</p> <p>También debe asegurarse de que la directiva esté actualizada a medida que se añadan nuevos permisos en versiones posteriores.</p>	"Permisos de Azure para Connector"

Permisos de Google Cloud

Específico	Descripción	Enlace
Despliegue del conector	El usuario de Google Cloud que implementa un conector de BlueXP necesita permisos específicos para implementar el conector en Google Cloud.	"Configure los permisos para desplegar el conector"
Funcionamiento del conector	La cuenta de servicio de la instancia de Connector VM debe tener permisos específicos para las operaciones del día a día. Debe asociar la cuenta de servicio al conector cuando la despliegue desde BlueXP. También debe asegurarse de que la directiva esté actualizada a medida que se añadan nuevos permisos en versiones posteriores.	"Configure una cuenta de servicio para el conector"

Permisos de AWS para Connector

Cuando BlueXP inicia la instancia de Connector en AWS, asocia una directiva a la instancia que proporciona al conector permisos para administrar recursos y procesos dentro de esa cuenta de AWS. El conector utiliza los permisos para realizar llamadas API a varios servicios de AWS, incluidos EC2, S3, CloudFormation, IAM, El Servicio de gestión de claves (KMS), etc.

Políticas IAM

Las políticas de IAM disponibles a continuación proporcionan los permisos que un conector necesita para gestionar recursos y procesos dentro de su entorno de cloud público basado en su región de AWS.

Si crea un conector en una región estándar de AWS directamente desde BlueXP, BlueXP aplica automáticamente directivas al conector. En este caso no es necesario hacer nada.

Si pone en marcha el conector desde AWS Marketplace o si instala manualmente el conector en un host Linux, deberá configurar las políticas usted mismo.

También debe asegurarse de que las directivas estén actualizadas a medida que se añadan nuevos permisos

en versiones posteriores.

Seleccione su región para ver las políticas necesarias:

Regiones estándar

Para las regiones estándar, los permisos se distribuyen en dos directivas. Son necesarias dos políticas debido a un límite máximo de tamaño de carácter para las políticas gestionadas en AWS.

La primera directiva proporciona permisos para los siguientes servicios:

- Backup en el cloud
- Cloud Data SENSE
- Organización en niveles del cloud
- Cloud Volumes ONTAP
- FSX para ONTAP
- Detección de bloques de S3

La segunda directiva proporciona permisos para los siguientes servicios:

- Etiquetado de AppTemplate
- Caché de archivos global
- Kubernetes

Política #1

```
{
  "Statement": [
    {
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:CreatePlacementGroup",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateRoute",
        "ec2:DescribeVpcs",
        "ec2:ReplaceRoute",
        "ec2:UnassignPrivateIpAddresses",
        "ec2>DeleteSecurityGroup",
```

```
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"ec2:DescribePlacementGroups",
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
"cloudformation:CreateStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"cloudformation:DeleteStack",
"iam:PassRole",
"iam:CreateRole",
"iam:PutRolePolicy",
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:ListInstanceProfiles",
"iam:DeleteRole",
"iam:DeleteRolePolicy",
"iam:DeleteInstanceProfile",
"iam:GetRolePolicy",
"iam:GetRole",
"sts:DecodeAuthorizationMessage",
"sts:AssumeRole",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:CreateBucket",
"s3:GetLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketPolicy",
"s3:GetBucketAcl",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"s3:DeleteObject",
"s3:DeleteObjectVersion",
"s3:PutObject",
"s3:ListAllMyBuckets",
"s3:GetObject",
"s3:GetEncryptionConfiguration",
"kms:List*",
```

```

        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "fsx:Describe*",
        "fsx:List*"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "cvoServicePolicy"
},
{
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceState",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "kms:List*",
        "kms:Describe*",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
    ]
}

```



```

        "glue:BatchDeletePartition"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "backupPolicy"
},
{
    "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectRetention",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:BypassGovernanceRetention",
        "s3:PutBucketPolicy",
        "s3:PutBucketOwnershipControls"
    ],
    "Resource": [

```

```

        "arn:aws:s3:::netapp-backup-*"
    ],
    "Effect": "Allow",
    "Sid": "backupS3Policy"
},
{
    "Action": [
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3>DeleteBucket"
    ],
    "Resource": [
        "arn:aws:s3:::fabric-pool*"
    ],
    "Effect": "Allow",
    "Sid": "fabricPoolS3Policy"
},
{
    "Action": [
        "ec2:DescribeRegions"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "fabricPoolPolicy"
},
{
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/netapp-adc-manager": "*"
        }
    },
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}

```

```

    ],
    "Effect": "Allow"
  },
  {
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/WorkingEnvironment": "*"
      }
    },
    "Action": [
      "ec2:StartInstances",
      "ec2:TerminateInstances",
      "ec2:AttachVolume",
      "ec2:DetachVolume",
      "ec2:StopInstances",
      "ec2>DeleteVolume"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "ec2:AttachVolume",
      "ec2:DetachVolume"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Effect": "Allow"
  },
  {
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/WorkingEnvironment": "*"
      }
    },
    "Action": [
      "ec2>DeleteVolume"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Effect": "Allow"
  }
}

```

```
]
}
```

Política #2

```
{
  "Statement": [
    {
      "Action": [
        "ec2:DescribeRegions",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "K8sServicePolicy"
    },
    {
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "GFCservicePolicy"
    },
    {
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/GFCInstance": "*"
        }
      },
      "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Effect": "Allow"
    },
    {
```

```
    "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "tagServicePolicy"
}
]
```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListInstanceProfiles",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "ec2:ModifyVolumeAttribute",
        "sts:DecodeAuthorizationMessage",
        "ec2:DescribeImages",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstances",
        "iam:PassRole",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2>DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2>DeleteSnapshot",

```

```

        "ec2:DescribeSnapshots",
        "ec2:StopInstances",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3>DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",

```

```

        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::fabric-pool*"
    ]
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::netapp-backup-*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {

```



```

        "ec2:ResourceTag/WorkingEnvironment": "*"
    },
    "Resource": [
        "arn:aws-us-gov:ec2:*:*:instance/*"
    ],
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:volume/*"
        ]
    }
]
}

```

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
      "iam:PassRole",

```

```

        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",

```

```

        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}
]
}

```

Cómo se utilizan los permisos de AWS

En las siguientes secciones se describe cómo se utilizan los permisos para cada servicio cloud de NetApp. Esta información puede ser útil si sus políticas corporativas dictan que los permisos sólo se proporcionan según sea necesario.

Etiquetas de AppTemplate

El conector realiza las siguientes solicitudes de API para administrar etiquetas en recursos de AWS cuando utiliza el servicio de etiquetado AppTemplate:

- ec2:CreateTags
- ec2>DeleteTags
- ec2:etiquetas a describTags
- Tag:getResources
- Etiqueta:getTagKeys
- Etiqueta:getTagValues
- Tag:TagResources
- Tag:UntagResources

Backup en el cloud

El conector realiza las siguientes solicitudes API para implementar la instancia de restauración para Cloud Backup:

- ec2:StartInstances
- ec2:StopInstances
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:DescribeInstanceAttribute
- ec2:DescribeImages
- ec2:CreateTags
- ec2:CreateVolume
- ec2:CreateSecurityGroup
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:regiones describidas
- Cloudformation:CreateStack
- Cloudformation>DeleteStack
- Cloudformation:DescribeStacks

El conector realiza las siguientes solicitudes API para gestionar backups en Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketEncryption
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Kms:List*
- Kms:describe*
- s3:GetObject
- ec2:DescribeVpcEndpoints
- Kms:ListAliases

- s3:PutEncryptionConfiguration

El conector realiza las siguientes solicitudes API cuando utiliza el método Search & Restore para restaurar volúmenes y archivos:

- s3:CreateBucket
- s3>DeleteObject
- s3>DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Cola:CreateDatabase
- Pegar>CreateTable
- Cola:BatchDeletePartition

El conector realiza las siguientes solicitudes de API al usar la protección DataLock y ransomware para los backups de volúmenes:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectEtiquetado
- s3>DeleteObject
- s3>DeleteObjectTagging
- s3:GetObjectRetention
- s3>DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration

- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketEtiquetado
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionEtiquetado
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

El conector realiza las siguientes solicitudes de API si utiliza una cuenta de AWS diferente para los backups de Cloud Volumes ONTAP de la que usa en los volúmenes de origen:

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

Cloud Data SENSE

El conector realiza las siguientes solicitudes de API para implementar la instancia de Cloud Data Sense:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2>DeleteSecurityGroup
- ec2:DescribeSecurityGroups
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkinterfaces
- ec2>DeleteNetworkInterface
- ec2:DescribeSubnets

- ec2:DescribeVpcs
- ec2:CreateSnapshot
- ec2:regiones descritas
- Cloudformation:CreateStack
- Cloudformation>DeleteStack
- Cloudformation:DescribeStacks
- Cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

El conector realiza las siguientes solicitudes de API para analizar bloques de S3 cuando utiliza Cloud Data Sense:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3>DeleteObject
- s3>DeleteObjectVersion
- s3:PutObject
- sts:AssumeRole

Organización en niveles del cloud

El conector realiza las siguientes solicitudes de API para organizar los datos en niveles en Amazon S3 cuando se utiliza Cloud Tiering.

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
s3:CreateBucket	Sí	No
s3:PutLifecycleConfiguration	Sí	No
s3:GetLifecycleConfiguration	Sí	Sí

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
ec2:regiones descritas	Sí	No
ec2:DescribeVpcEndpoints	Sí	No

Cloud Volumes ONTAP

El conector realiza las siguientes solicitudes de API para implementar y gestionar Cloud Volumes ONTAP en AWS.

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Crear y gestionar roles e perfiles de instancia de IAM para instancias de Cloud Volumes ONTAP	iam:ListInstanceProfiles	Sí	Sí	No
	iam:CreateRole	Sí	No	No
	iam>DeleteRole	No	Sí	Sí
	iam:PutRolePolicy	Sí	No	No
	iam:CreateInstanceProfile	Sí	No	No
	iam>DeleteRolePolicy	No	Sí	Sí
	iam:AddRoleToInstanceProfile	Sí	No	No
	iam:RemoveRoleFromInstanceProfile	No	Sí	Sí
	iam>DeleteInstanceProfile	No	Sí	Sí
	iam:PassRole	Sí	No	No
	ec2:AssociateIamInstanceProfile	Sí	Sí	No
	ec2:DescribeIamInstanceProfileAssociations	Sí	Sí	No
	ec2:DisassociateIamInstanceProfile	No	Sí	No
Decodificar mensajes de estado de autorización	sts:DecodeAuthorizationMessage	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Describa las imágenes especificadas (AMI) disponibles para la cuenta	ec2:DescribeImages	Sí	Sí	No
Describir las tablas de rutas en un VPC (solo necesarias para los pares de alta disponibilidad)	ec2:DescribeRouteTables	Sí	No	No
Detener, iniciar y supervisar instancias	ec2:StartInstances	Sí	Sí	No
	ec2:StopInstances	Sí	Sí	No
	ec2:DescribeInstances	Sí	Sí	No
	ec2:DescribeInstanceStatus	Sí	Sí	No
	ec2:RunInstances	Sí	No	No
	ec2:TerminateInstances	No	No	Sí
	ec2:ModifyInstanceAttribute	No	Sí	No
Compruebe que las redes mejoradas estén habilitadas para los tipos de instancia compatibles	ec2:DescribeInstanceAttribute	No	Sí	No
Etiquete los recursos con las etiquetas "WorkingEnvironment" y "WorkingEnvironmentId" que se utilizan para el mantenimiento y la asignación de costes	ec2:CreateTags	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Gestione volúmenes de EBS que Cloud Volumes ONTAP utiliza como almacenamiento back-end	ec2:CreateVolume	Sí	Sí	No
	ec2:DescribeVolumes	Sí	Sí	Sí
	ec2:ModifyVolumeAttribute	No	Sí	Sí
	ec2:AttachVolume	Sí	Sí	No
	ec2>DeleteVolume	No	Sí	Sí
	ec2:DetachVolume	No	Sí	Sí
Crear y administrar grupos de seguridad para Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Sí	No	No
	ec2>DeleteSecurityGroup	No	Sí	Sí
	ec2:DescribeSecurityGroups	Sí	Sí	Sí
	ec2:RevokeSecurityGroupEgress	Sí	No	No
	ec2:AuthorizeSecurityGroupEgress	Sí	No	No
	ec2:AuthorizeSecurityGroupIngress	Sí	No	No
	ec2:RevokeSecurityGroupIngress	Sí	Sí	No
Cree y gestione interfaces de red para Cloud Volumes ONTAP en la subred de destino	ec2:CreateNetworkInterface	Sí	No	No
	ec2:DescribeNetworkInterfaces	Sí	Sí	No
	ec2>DeleteNetworkInterface	No	Sí	Sí
	ec2:ModifyNetworkInterfaceAttribute	No	Sí	No
Obtenga la lista de subredes de destino y grupos de seguridad	ec2:DescribeSubnets	Sí	Sí	No
	ec2:DescribeVpcs	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Obtenga los servidores DNS y el nombre de dominio predeterminado para las instancias de Cloud Volumes ONTAP	ec2:DescribeDhcpOptions	Sí	No	No
Tome snapshots de volúmenes de EBS para Cloud Volumes ONTAP	ec2:CreateSnapshot	Sí	Sí	No
	ec2:DeleteSnapshot	No	Sí	Sí
	ec2:DescribeSnapshots	No	Sí	No
Capture la consola Cloud Volumes ONTAP, que está conectada a mensajes de AutoSupport	ec2:GetConsoleOutput	Sí	Sí	No
Obtenga la lista de pares de claves disponibles	ec2:DescribeKeyPairs	Sí	No	No
Obtenga la lista de regiones disponibles de AWS	ec2:regions	Sí	Sí	No
Gestione etiquetas para los recursos asociados a instancias de Cloud Volumes ONTAP	ec2:DeleteTags	No	Sí	Sí
	ec2:etiquetas a describTags	No	Sí	No
Cree y administre pilas para plantillas CloudFormation de AWS	Cloudformation:CreateStack	Sí	No	No
	Cloudformation:DeleteStack	Sí	No	No
	Cloudformation:DescribeStacks	Sí	Sí	No
	Cloudformation:DescribeStackEvents	Sí	No	No
	Cloudformation:ValidateTemplate	Sí	No	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione un bloque de S3 que un sistema Cloud Volumes ONTAP utiliza como nivel de capacidad para la organización en niveles de datos	s3:CreateBucket	Sí	Sí	No
	s3:DeleteBucket	No	Sí	Sí
	s3:GetLifecycleConfiguration	No	Sí	No
	s3:PutLifecycleConfiguration	No	Sí	No
	s3:PutBucketEncryption	No	Sí	No
	s3:ListBucketVersions	No	Sí	No
	s3:GetBucketPolicyStatus	No	Sí	No
	s3:GetBucketPublicAccessBlock	No	Sí	No
	s3:GetBucketAcl	No	Sí	No
	s3:GetBucketPolicy	No	Sí	No
	s3:PutBucketPublicAccessBlock	No	Sí	No
	s3:GetBucketTagging	No	Sí	No
	s3:GetBucketLocation	No	Sí	No
	s3:ListAllMyBuckets	No	No	No
	s3:ListBucket	No	Sí	No
Habilitar el cifrado de datos de Cloud Volumes ONTAP mediante el servicio de gestión de claves (KMS) de AWS	Kms:Lista*	Sí	Sí	No
	Kms:Recifrar*	Sí	No	No
	Kms:describir*	Sí	Sí	No
	Kms:CreateGrant	Sí	Sí	No
Obtenga datos de coste de AWS para Cloud Volumes ONTAP	ce:GetReservationUtilization	No	Sí	No
	ce:GetDimensionValues	No	Sí	No
	ce:GetCostAndUsage	No	Sí	No
	ce:getTags	No	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione un grupo de colocación extendido de AWS para dos nodos de alta disponibilidad y el mediador en una única zona de disponibilidad de AWS	ec2:CreatePlacementGroup	Sí	No	No
	ec2:DeletePlacementGroup	No	Sí	Sí
Crear informes	fsx:describe*	No	Sí	No
	fsx:List*	No	Sí	No
Cree y gestione agregados que admitan la función Amazon EBS Elastic Volumes	ec2:DescribeVolumesModificaciones	No	Sí	No
	ec2:ModifyVolume	No	Sí	No

Caché de archivos global

El conector realiza las siguientes solicitudes de API para implementar instancias de caché de archivos global durante la implementación:

- Cloudformation:DescribeStacks
- Cloudwatch:GetMetricStatistics
- Cloudformation:ListStacks

FSX para ONTAP

El conector realiza las siguientes solicitudes de API para administrar FSX para ONTAP:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeDhcpOptions

- ec2:DescribeSnapshots
- ec2:DescribeKeyPairs
- ec2:regiones descritas
- ec2:etiquetas a describTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribeVolumesModificaciones
- ec2:DescribePlacementGroups
- Kms:Lista*
- Kms:describir*
- Kms>CreateGrant
- Kms:ListAliases
- fsx:describe*
- fsx:List*

Kubernetes

El conector realiza las siguientes solicitudes de API para detectar y gestionar clústeres de Amazon EKS:

- ec2:regiones descritas
- eks:ListClusters
- eks:DescribeCluster
- iam:GetInstanceProfile

Detección de bloques de S3

El conector hace la siguiente solicitud de API para detectar bloques de Amazon S3:

s3:GetEncryptionConfiguration

Registro de cambios

A medida que se añadan y eliminen permisos, los anotaremos en las secciones siguientes.

14 de febrero de 2023

Ahora se necesita el siguiente permiso para la organización en niveles del cloud:

ec2:DescribeVpcEndpoints

Permisos de Azure para Connector

Cuando BlueXP inicia Connector VM en Azure, asocia una función personalizada a la máquina virtual que proporciona al conector permisos para gestionar recursos y

procesos en esa suscripción a Azure. El conector utiliza los permisos para realizar llamadas API a varios servicios de Azure.

Permisos de roles personalizados

El rol personalizado que se muestra a continuación proporciona los permisos que un conector necesita para administrar recursos y procesos dentro de su red de Azure.

Al crear un conector directamente desde BlueXP, BlueXP aplica automáticamente esta función personalizada al conector.

Si pone en marcha el conector desde Azure Marketplace o si instala manualmente el conector en un host Linux, deberá configurar el rol personalizado usted mismo.

También debe asegurarse de que el rol esté actualizado a medida que se añadan nuevos permisos en versiones posteriores.

```
{
  "Name": "BlueXP Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
```



```
"Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",
    "Microsoft.Storage/storageAccounts/listkeys/action",
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/write",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
    "Microsoft.Storage/usages/read",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/read",
    "Microsoft.Compute/availabilitySets/write",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",

    "Microsoft.Network/loadBalancers/read",
```

```
"Microsoft.Network/loadBalancers/write",
"Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
    "Microsoft.Network/loadBalancers/probes/read",
    "Microsoft.Network/loadBalancers/probes/join/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Network/routeTables/join/action",
    "Microsoft.NetApp/netAppAccounts/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
    "Microsoft.Network/privateEndpoints/read",
    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/privateDnsZones/A/write",
    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/delete",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
```

```

        "Microsoft.Network/networkInterfaces/delete",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Resources/deployments/delete",
        "Microsoft.Compute/diskEncryptionSets/read",
        "Microsoft.Compute/snapshots/delete",
        "Microsoft.Network/privateEndpoints/delete",
        "Microsoft.Compute/availabilitySets/delete",
        "Microsoft.KeyVault/vaults/read",
        "Microsoft.KeyVault/vaults/accessPolicies/write",
        "Microsoft.Compute/diskEncryptionSets/write",
        "Microsoft.KeyVault/vaults/deploy/action",
        "Microsoft.Compute/diskEncryptionSets/delete",
        "Microsoft.Resources/tags/read",
        "Microsoft.Resources/tags/write",
        "Microsoft.Resources/tags/delete",
        "Microsoft.Network/applicationSecurityGroups/write",
        "Microsoft.Network/applicationSecurityGroups/read",

        "Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/applicationSecurityGroups/delete",

        "Microsoft.Network/networkSecurityGroups/securityRules/delete",

        "Microsoft.ContainerService/managedClusters/listClusterUserCredential/action",

        "Microsoft.ContainerService/managedClusters/read",
        "Microsoft.Synapse/workspaces/write",
        "Microsoft.Synapse/workspaces/read",
        "Microsoft.Synapse/workspaces/delete",
        "Microsoft.Synapse/register/action",
        "Microsoft.Synapse/checkNameAvailability/action",
        "Microsoft.Synapse/workspaces/operationStatuses/read",
        "Microsoft.Synapse/workspaces/firewallRules/read",

        "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
        "Microsoft.Synapse/workspaces/operationResults/read",
        "Microsoft.Network/publicIPAddresses/delete",

        "Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

        "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
    ],
    "NotActions": [],
    "AssignableScopes": [],

```

```
"Description": "BlueXP Permissions",  
"IsCustom": "true"  
}
```

Cómo se utilizan los permisos de Azure

En las siguientes secciones se describe cómo se utilizan los permisos para cada servicio cloud de NetApp. Esta información puede ser útil si sus políticas corporativas dictan que los permisos sólo se proporcionan según sea necesario.

Etiquetas de AppTemplate

El conector realiza las siguientes solicitudes de API para administrar etiquetas en recursos de Azure cuando utiliza el servicio de etiquetado AppTemplate:

- Microsoft.Resources/resources/read
- Microsoft.Resources/subscripciones/operationResults/read
- Microsoft.Resources/subscriptions/ResourceGroups/read
- Microsoft.Resources/subscripciones/resourcegroups/resources/read
- Microsoft.Resources/etiquetas/leer
- Microsoft.Resources/etiquetas/escritura

Azure NetApp Files

El conector realiza las siguientes solicitudes de API para gestionar entornos de trabajo de Azure NetApp Files:

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

Backup en el cloud

El conector realiza las siguientes solicitudes de API para operaciones de backup y restauración:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/Write
- Microsoft.Storage/storageAccounts/blobServices/contenedores/lectura
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.KeyVault/vaults/read

- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/suscripciones/ubicaciones/leer
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/subscriptions/ResourceGroups/read
- Microsoft.Resources/subscripciones/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/ResourceGroups/write
- Microsoft.Authorization/locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/despliegues/DELETE
- Microsoft.Network/publicIPAddresses/delete
- Microsoft.Storage/storageAccounts/blobServices/contenedores/escritura
- Microsoft.ManagedIdentity/userAssignedIdentities/ASSIGN/action

El conector realiza las siguientes solicitudes de API cuando utiliza la funcionalidad Buscar y restaurar:

- Microsoft.Synapse/Sáreas de trabajo/escritura
- Microsoft.Synapse/áreas de trabajo/lectura
- Microsoft.Synapse/áreas de trabajo/eliminar
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/Action
- Microsoft.Synapse/Sáreas de trabajo/operationStatuses/Read
- Microsoft.Synapse/áreas de trabajo/firewallRules/read
- Microsoft.Synapse/spaces/replaceAllIpFirewallRules/acción
- Microsoft.Synapse/áreas de trabajo/operationResults/read
- Microsoft.Synapse/spots/privateEndpointConnectionsApproval/action

Cloud Data SENSE

El conector realiza las siguientes solicitudes de API cuando utiliza Cloud Data Sense.

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Compute/locations/operations/read	Sí	Sí
Microsoft.Compute/locations/vmSizes/read	Sí	Sí
Microsoft.Compute/operations/read	Sí	Sí
Microsoft.Compute/virtualMachines/instanceView/read	Sí	Sí
Microsoft.Compute/virtualMachines/powerOff/action	Sí	No
Microsoft.Compute/virtualMachines/read	Sí	Sí
Microsoft.Compute/virtualMachines/restart/action	Sí	No
Microsoft.Compute/virtualMachines/start/action	Sí	No
Microsoft.Compute/virtualMachines/vmSizes/read	No	Sí
Microsoft.Compute/virtualMachines/write	Sí	No
Microsoft.Compute/images/read	Sí	Sí
Microsoft.Compute/disks/delete	Sí	No
Microsoft.Compute/disks/read	Sí	Sí
Microsoft.Compute/disks/write	Sí	No
Microsoft.Storage/checknameavailability/leer	Sí	Sí
Microsoft.almacenamiento/operaciones/lectura	Sí	Sí
Microsoft.Storage/storageAccounts/listkeys/action	Sí	No
Microsoft.Storage/storageAccounts/read	Sí	Sí
Microsoft.Storage/storageAccounts/Write	Sí	No
Microsoft.Storage/storageAccounts/DELETE	No	Sí

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Storage/storageAccounts/blobServices/contenedores/lectura	Sí	Sí
Microsoft.Network/networkInterfaces/read	Sí	Sí
Microsoft.Network/networkInterfaces/write	Sí	No
Microsoft.Network/networkInterfaces/join/action	Sí	No
Microsoft.Network/networkSecurityGroups/read	Sí	Sí
Microsoft.Network/networkSecurityGroups/write	Sí	No
Microsoft.Resources/suscripciones/ubicaciones/leer	Sí	Sí
Microsoft.Network/locations/operationResults/read	Sí	Sí
Microsoft.Network/locations/operations/read	Sí	Sí
Microsoft.Network/virtualNetworks/read	Sí	Sí
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Sí	Sí
Microsoft.Network/virtualNetworks/subnets/read	Sí	Sí
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Sí	Sí
Microsoft.Network/virtualNetworks/virtualMachines/read	Sí	Sí
Microsoft.Network/virtualNetworks/subnets/join/action	Sí	No
Microsoft.Network/virtualNetworks/subnets/write	Sí	No
Microsoft.Network/routeTables/join/action	Sí	No
Microsoft.Resources/despliegues/operaciones/lectura	Sí	Sí
Microsoft.Resources/despliegues/leer	Sí	Sí
Microsoft.Resources/implementaciones/escritura	Sí	No

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Resources/resources/read	Sí	Sí
Microsoft.Resources/subscriptions/operationResults/read	Sí	Sí
Microsoft.Resources/subscriptions/ResourceGroups/delete	Sí	No
Microsoft.Resources/subscriptions/ResourceGroups/read	Sí	Sí
Microsoft.Resources/subscriptions/resourcegroups/resources/read	Sí	Sí
Microsoft.Resources/subscriptions/ResourceGroups/write	Sí	No

Organización en niveles del cloud

El conector realiza las siguientes solicitudes de API al configurar Cloud Tiering.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/subscriptions/ResourceGroups/read
- Microsoft.Resources/subscriptions/ubicaciones/leer

El conector realiza las siguientes solicitudes API para operaciones diarias.

- Microsoft.Storage/storageAccounts/blobServices/contenedores/lectura
- Microsoft.Storage/storageAccounts/blobServices/contenedores/escritura
- Microsoft.Storage/storageAccounts/managementPolicies/Read
- Microsoft.Storage/storageAccounts/managementPolicies/Write
- Microsoft.Storage/storageAccounts/read

Cloud Volumes ONTAP

El conector realiza las siguientes solicitudes de API para implementar y gestionar Cloud Volumes ONTAP en Azure.

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree las máquinas virtuales, pare, inicie, elimine y obtenga el estado del sistema	Microsoft.Compute/locations/operations/read	Sí	Sí	No
	Microsoft.Compute/locations/vmSizes/read	Sí	Sí	No
	Microsoft.Resources/suscripciones/ubicaciones/leer	Sí	No	No
	Microsoft.Compute/operations/read	Sí	Sí	No
	Microsoft.Compute/virtualMachines/instanceView/read	Sí	Sí	No
	Microsoft.Compute/virtualMachines/powerOff/action	Sí	Sí	No
	Microsoft.Compute/virtualMachines/read	Sí	Sí	No
	Microsoft.Compute/virtualMachines/restart/action	Sí	Sí	No
	Microsoft.Compute/virtualMachines/start/action	Sí	Sí	No
	Microsoft.Compute/virtualMachines/deallocate/action	No	Sí	Sí
	Microsoft.Compute/virtualMachines/vmSizes/read	No	Sí	No
	Microsoft.Compute/virtualMachines/write	Sí	Sí	No
Habilite la puesta en marcha desde un disco duro virtual	Microsoft.Compute/images/read	Sí	No	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione interfaces de red en la subred de destino	Microsoft.Network/networkInterfaces/read	Sí	Sí	No
	Microsoft.Network/networkInterfaces/write	Sí	Sí	No
	Microsoft.Network/networkInterfaces/join/action	Sí	Sí	No
Crear grupos de seguridad de red predefinidos	Microsoft.Network/networkSecurityGroups/read	Sí	Sí	No
	Microsoft.Network/networkSecurityGroups/write	Sí	Sí	No
	Microsoft.Network/networkSecurityGroups/join/action	Sí	No	No
Obtenga información de la red acerca de las regiones, la red virtual de destino y la subred, y agregue las máquinas virtuales a los VNets	Microsoft.Network/locations/operationResults/read	Sí	Sí	No
	Microsoft.Network/locations/operations/read	Sí	Sí	No
	Microsoft.Network/virtualNetworks/read	Sí	No	No
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Sí	No	No
	Microsoft.Network/virtualNetworks/subnets/read	Sí	Sí	No
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Sí	Sí	No
	Microsoft.Network/virtualNetworks/virtualMachines/read	Sí	Sí	No
	Microsoft.Network/virtualNetworks/subnets/join/action	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione grupos de recursos	Microsoft.Resources /despliegues/operaciones/lectura	Sí	Sí	No
	Microsoft.Resources /despliegues/leer	Sí	Sí	No
	Microsoft.Resources /implementaciones/escritura	Sí	Sí	No
	Microsoft.Resources /resources/read	Sí	Sí	No
	Microsoft.Resources /subscripciones/operationResults/read	Sí	Sí	No
	Microsoft.Resources /subscriptions/ResourceGroups/delete	Sí	Sí	Sí
	Microsoft.Resources /subscriptions/ResourceGroups/read	No	Sí	No
	Microsoft.Resources /subscripciones/resourcegroups/resources/read	Sí	Sí	No
	Microsoft.Resources /subscriptions/ResourceGroups/write	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Gestione cuentas de almacenamiento de Azure y discos	Microsoft.Compute/disks/read	Sí	Sí	Sí
	Microsoft.Compute/disks/write	Sí	Sí	No
	Microsoft.Compute/disks/delete	Sí	Sí	Sí
	Microsoft.Storage/checknameavailability/peer	Sí	Sí	No
	Microsoft.almacenamiento/operaciones/lectura	Sí	Sí	No
	Microsoft.Storage/storageAccounts/listkeys/action	Sí	Sí	No
	Microsoft.Storage/storageAccounts/read	Sí	Sí	No
	Microsoft.Storage/storageAccounts/DELETE	No	Sí	Sí
	Microsoft.Storage/storageAccounts/Write	Sí	Sí	No
	Microsoft.almacenamiento/usuarios/lectura	No	Sí	No
Permita los backups al almacenamiento BLOB y el cifrado de cuentas de almacenamiento	Microsoft.Storage/storageAccounts/blobServices/containers/lectura	Sí	Sí	No
	Microsoft.KeyVault/vaults/read	Sí	Sí	No
	Microsoft.KeyVault/vaults/accessPolicies/write	Sí	Sí	No
Habilite extremos de servicio vnet para la organización en niveles de los datos	Microsoft.Network/virtualNetworks/subnets/write	Sí	Sí	No
	Microsoft.Network/routeTables/join/action	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Cree y gestione copias Snapshot gestionadas de Azure	Microsoft.Compute/snapshots/write	Sí	Sí	No
	Microsoft.Compute/snapshots/read	Sí	Sí	No
	Microsoft.Compute/snapshots/delete	No	Sí	Sí
	Microsoft.Compute/disks/beginGetAccess/action	No	Sí	No
Crear y gestionar conjuntos de disponibilidad	Microsoft.Compute/availabilitySets/write	Sí	No	No
	Microsoft.Compute/availabilitySets/read	Sí	No	No
Permita puestas en marcha programáticas desde el mercado	Microsoft.MarketplaceOrdering/offertypes/editores/ofertas/planes/acuerdos/leer	Sí	No	No
	Microsoft.MarketplaceOrdering/offertypes/editores/ofertas/planes/acuerdos/escribir	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Gestione un equilibrador de carga para pares de ha	Microsoft.Network/loadBalancers/read	Sí	Sí	No
	Microsoft.Network/loadBalancers/write	Sí	No	No
	Microsoft.Network/loadBalancers/delete	No	Sí	Sí
	Microsoft.Network/loadBalancers/backendAddressPools/read	Sí	Sí	No
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Sí	No	No
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Sí	No	No
	Microsoft.Network/loadBalancers/probes/read	Sí	No	No
	Microsoft.Network/loadBalancers/probes/join/action	Sí	No	No
Habilite la gestión de bloqueos en discos de Azure	Microsoft.Authorization/locks/*	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Habilite extremos privados para pares de alta disponibilidad cuando no haya conectividad fuera de la subred	Microsoft.Network/privateEndpoints/write	Sí	Sí	No
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Sí	No	No
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	Sí	Sí	Sí
	Microsoft.Network/privateEndpoints/read	Sí	Sí	Sí
	Microsoft.Network/privateDnsZones/write	Sí	Sí	No
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Sí	Sí	No
	Microsoft.Network/virtualNetworks/join/action	Sí	Sí	No
	Microsoft.Network/privateDnsZones/A/write	Sí	Sí	No
	Microsoft.Network/privateDnsZones/read	Sí	Sí	No
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Sí	Sí	No
Lo requiere Azure para algunas puestas en marcha de máquinas virtuales, en función del hardware físico subyacente	Microsoft.Resources/despliegues/operationStatuses/read	Sí	Sí	No
Quite recursos de un grupo de recursos en caso de un error de implementación o de su eliminación	Microsoft.Network/privateEndpoints/delete	Sí	Sí	No
	Microsoft.Compute/availabilitySets/delete	Sí	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Habilite el uso de claves de cifrado gestionadas por el cliente al usar la API	Microsoft.Compute/diskEncryptionSets/read	Sí	Sí	Sí
	Microsoft.Compute/diskEncryptionSets/write	Sí	Sí	No
	Microsoft.KeyVault/vaults/Deploy/action	Sí	No	No
	Microsoft.Compute/diskEncryptionSets/delete	Sí	Sí	Sí
Configurar un grupo de seguridad de aplicaciones para un par de alta disponibilidad para aislar las NIC de interconexión de alta disponibilidad y de red de clúster	Microsoft.Network/applicationSecurityGroups/write	No	Sí	No
	Microsoft.Network/applicationSecurityGroups/read	No	Sí	Sí
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	No	Sí	No
	Microsoft.Network/networkSecurityGroups/securityRules/write	Sí	Sí	No
	Microsoft.Network/applicationSecurityGroups/delete	No	Sí	No
	Microsoft.Network/networkSecurityGroups/securityRules/delete	No	Sí	Sí
Lea, escriba y elimine las etiquetas asociadas a los recursos de Cloud Volumes ONTAP	Microsoft.Resources/etiquetas/leer	No	Sí	No
	Microsoft.Resources/etiquetas/escritura	Sí	Sí	No
	Microsoft.Resources/etiquetas/eliminar	Sí	No	No
Cifre cuentas de almacenamiento durante la creación	Microsoft.ManagedIdentity/userAssignedIdentities/ASSIGN/action	Sí	Sí	No

Caché de archivos global

El conector realiza las siguientes solicitudes API cuando utiliza la caché de archivos global:

- Microsoft.Insights/Metrics/Read
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/despliegues/DELETE

Kubernetes

El conector realiza las siguientes solicitudes de API para detectar y gestionar clústeres que se ejecutan en Azure Kubernetes Service (AKS):

- Microsoft.Compute/virtualMachines/read
- Microsoft.Resources/suscripciones/ubicaciones/leer
- Microsoft.Resources/subscripciones/operationResults/read
- Microsoft.Resources/subscriptions/ResourceGroups/read
- Microsoft.Resources/subscripciones/resourcegroups/resources/read
- Microsoft.ContainerService/managedClusters/read
- Microsoft.ContainerService/managedClusters/listClusterUserCredential/acción

Registro de cambios

A medida que se añadan y eliminen permisos, los anotaremos en las secciones siguientes.

5 de enero de 2023

Se han agregado los siguientes permisos a la política de JSON:

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/spots/privateEndpointConnectionsApproval/action

Estos permisos son necesarios para Cloud Backup.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

Este permiso es necesario para la implementación de Cloud Volumes ONTAP.

1 de diciembre de 2022

Se han agregado los siguientes permisos a la política de JSON:

- Microsoft.Storage/storageAccounts/blobServices/contenedores/escritura

Este permiso es necesario para Cloud Backup y Cloud Tiering.

- Microsoft.Network/publicIPAddresses/delete

Estos permisos son necesarios para Cloud Backup.

Se han eliminado los siguientes permisos de la política JSON porque ya no son necesarios:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read
- Microsoft.Storage/storageAccounts/regeneratekey/acción

Permisos de Google Cloud para Connector

BlueXP requiere permisos para realizar acciones en Google Cloud. Estos permisos se incluyen en un rol personalizado que proporciona NetApp. Puede que desee entender lo que BlueXP hace con estos permisos.

Permisos de cuenta de servicio

La función personalizada que se muestra a continuación proporciona los permisos que un conector necesita para administrar recursos y procesos dentro de su red de Google Cloud.

Tendrá que aplicar esta función personalizada a una cuenta de servicio que se conecta a la máquina virtual del conector. ["Vea las instrucciones paso a paso"](#).

También debe asegurarse de que el rol esté actualizado a medida que se añadan nuevos permisos en versiones posteriores.

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
```

- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list

- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Cómo se utilizan los permisos de Google Cloud

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

Acciones	Específico
<ul style="list-style-type: none"> - deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifest.list - deploymentmanager.operators.get - deploymentmanager.operators.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.Types.get - deploymentmanager.types.list 	Para poner en marcha la instancia de máquina virtual de Cloud Volumes ONTAP mediante Google Cloud Deployment Manager.
- logEntries.list - logging.privateLogEntries.list	Para obtener unidades de registro de pila.
- resourceManager.projects.get	Para dar soporte a proyectos múltiples.
<ul style="list-style-type: none"> - storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update 	Para crear y gestionar un bucket de Google Cloud Storage para la organización de datos en niveles.
<ul style="list-style-type: none"> - cloudkms.cryptoKeyVersions.useToEncrypt - cloudKMS.cryptoKeys.get - cloudKMS.cryptoKeys.list - cloudKMS.Keyring.list 	Para utilizar claves de cifrado gestionadas por el cliente desde el Servicio de gestión de claves cloud con Cloud Volumes ONTAP.
<ul style="list-style-type: none"> - compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - Storage.objects.get - storage.objects.list 	Para establecer una cuenta de servicio en la instancia de Cloud Volumes ONTAP. Esta cuenta de servicio proporciona permisos para organizar los datos en niveles en un bloque de Google Cloud Storage.
- compute.ads.list	Para recuperar las direcciones de una región cuando se implementa un par de alta disponibilidad.
<ul style="list-style-type: none"> - Computar.backendServices.create - compuso.regionBackendServices.create - compuso.regionBackendServices.get - computar.regionBackendServices.list 	Para configurar un servicio back-end para distribuir el tráfico en un par de alta disponibilidad.
- compute.networks.updatePolicy	Para aplicar reglas de firewall en las PC y subredes para un par ha.
<ul style="list-style-type: none"> - compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig 	Para habilitar Cloud Data Sense.
- container.clusters.get - container.clusters.list	Para detectar los clústeres de Kubernetes que se ejecutan en Google Kubernetes Engine.
<ul style="list-style-type: none"> - compute.instanceGroups.get - computar.ads.get - compute.instances.updateNetworkInterface 	Crear y gestionar máquinas virtuales de almacenamiento en pares de alta disponibilidad de Cloud Volumes ONTAP.

Acciones	Específico
- Monitoring.timeries.list - Storage.buckets.getIamPolicy	Para descubrir información sobre cubos de Google Cloud Storage.
- CloudKMS.cryptocryKeys.get - cloudKMS.cryptocryKeys.getIamPolicy - cloudKMS.criptoKeyKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudKMS.Keyring.get - cloudKMS.Keyring.getIamPolicy - cloudKMS.Keyring.list - cloudkms.keyRings.setIamPolicy	Para seleccionar sus propias claves gestionadas por el cliente en el asistente de activación de Cloud Backup en lugar de usar las claves de cifrado predeterminadas gestionadas por Google.

Registro de cambios

A medida que se añadan y eliminen permisos, los anotaremos en las secciones siguientes.

6 de febrero de 2023

Se ha agregado el siguiente permiso a esta directiva:

- compute.instances.updateNetworkInterface

Este permiso es obligatorio para Cloud Volumes ONTAP.

27 de enero de 2023

Se han agregado los siguientes permisos a la directiva:

- CloudKMS.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- CloudKMS.Keyring.get
- CloudKMS.Keyring.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Estos permisos son necesarios para Cloud Backup.

Puertos

Reglas del grupo de seguridad en AWS

El grupo de seguridad de AWS para Connector requiere reglas tanto entrantes como salientes.

Reglas de entrada

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector

Protocolo	Puerto	Específico
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente a la interfaz de usuario local y conexiones desde la instancia de Cloud Data Sense
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp. Debe abrir manualmente este puerto después de la implementación. Obtenga más información sobre el servidor proxy del conector.
TCP	9060, 9061	Ofrece la capacidad de habilitar y utilizar Cloud Data Sense y Cloud Backup en puestas en marcha de cloud gubernamentales. Estos puertos también son necesarios para Cloud Backup si deshabilita la interfaz SaaS en su cuenta de BlueXP.

Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

Servicio	Protocolo	Puerto	Destino	Específico
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP, a Cloud Data Sense, a Ransomware servicio y a enviar mensajes de AutoSupport a NetApp

Servicio	Protocolo	Puerto	Destino	Específico
Llamadas API	TCP	3000	Mediador de alta disponibilidad de ONTAP	Comunicación con el mediador de alta disponibilidad de ONTAP
	TCP	8088	Backup en S3	Llamadas API a Backup en S3
DNS	UDP	53	DNS	Utilizado para resolver DNS por BlueXP

Reglas de grupos de seguridad en Azure

El grupo de seguridad de Azure para Connector requiere reglas tanto entrantes como salientes.

Reglas de entrada

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente a la interfaz de usuario local y conexiones desde la instancia de Cloud Data Sense
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp. Debe abrir manualmente este puerto después de la implementación. Obtenga más información sobre el servidor proxy del conector.
TCP	9060, 9061	Ofrece la capacidad de habilitar y utilizar Cloud Data Sense y Cloud Backup en puestas en marcha de cloud gubernamentales. Estos puertos también son necesarios para Cloud Backup si deshabilita la interfaz SaaS en su cuenta de BlueXP.

Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

Servicio	Protocolo	Puerto	Destino	Específico
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a Azure y ONTAP, a Cloud Data Sense, a servicio de ransomware y a envío de mensajes de AutoSupport a NetApp
DNS	UDP	53	DNS	Utilizado para resolver DNS por BlueXP

Reglas de firewall en Google Cloud

Las reglas de firewall de Google Cloud para el conector requieren reglas tanto entrantes como salientes.

Reglas de entrada

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Protocolo	Puerto	Específico
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp. Debe abrir manualmente este puerto después de la implementación. Obtenga más información sobre el servidor proxy del conector.

Reglas de salida

Las reglas de firewall predefinidas para el conector abren todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

Reglas de salida básicas

Las reglas de firewall predefinidas para el conector incluyen las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

Servicio	Protocolo	Puerto	Destino	Específico
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a GCP y ONTAP, al Cloud Data Sense, al servicio de ransomware y a envío de mensajes de AutoSupport a NetApp
DNS	UDP	53	DNS	Utilizado para resolver DNS por BlueXP

Puertos para el conector en las instalaciones

El conector utiliza los siguientes puertos *inbound* cuando se instalan manualmente en un host Linux local.

Estas reglas de entrada se aplican a ambos modelos de implementación para el conector en las instalaciones: Instalado con acceso a Internet o sin acceso a Internet.

Protocolo	Puerto	Específico
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Conocimiento y apoyo

Regístrese para recibir soporte

Antes de poder abrir un caso de soporte con el soporte técnico de NetApp, debe añadir una cuenta del sitio de soporte de NetApp (NSS) a BlueXP y, a continuación, registrarse para recibir soporte.

Soporte para soluciones de proveedores cloud

Para obtener asistencia técnica sobre las siguientes soluciones de proveedores de nube que ha integrado en BlueXP, consulte "obtención de ayuda" en la documentación de BlueXP para ese producto.

- ["Amazon FSX para ONTAP"](#)
- ["Azure NetApp Files"](#)
- ["Cloud Volumes Service para Google Cloud"](#)

Información general del registro de soporte

Existen dos formas de registro para activar el derecho de asistencia:

- Registro de la suscripción al soporte de ID de cuenta de BlueXP (número de serie de 20 dígitos xxxx960xxxxx que se encuentra en la página Recursos de asistencia técnica de BlueXP).

Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de BlueXP. Debe registrarse cada suscripción de asistencia técnica a nivel de cuenta de BlueXP.

- Registrar los números de serie de Cloud Volumes ONTAP asociados con una suscripción en el mercado de su proveedor de cloud (estos son números de serie de 20 dígitos 909201xxxxxxxx).

Estos números de serie se denominan comúnmente *PAYGO serial Numbers* y son generados por BlueXP en el momento de la implementación de Cloud Volumes ONTAP.

El registro de ambos tipos de números de serie permite funcionalidades, como abrir tickets de soporte y la generación automática de casos.

La forma de registrarse depende de si es un cliente o partner nuevo o existente.

- Cliente o partner existente

Como cliente o partner de NetApp, puede usar su cuenta de SSO del sitio de soporte de NetApp (NSS) para realizar estos registros anteriormente. En el Panel de soporte, BlueXP proporciona una página **NSS Management** en la que puede agregar su cuenta NSS. Una vez que agregue su cuenta NSS, BlueXP registra automáticamente estos números de serie.

[Aprenda a añadir su cuenta de NSS.](#)

- Nuevo en NetApp

Si es totalmente nuevo en NetApp, debe completar un registro una vez del número de serie de su ID de cuenta de BlueXP en el sitio de registro de soporte de NetApp. Una vez completado este registro y cree una nueva cuenta de NSS, puede utilizar esta cuenta en BlueXP para registrarse automáticamente en el futuro.

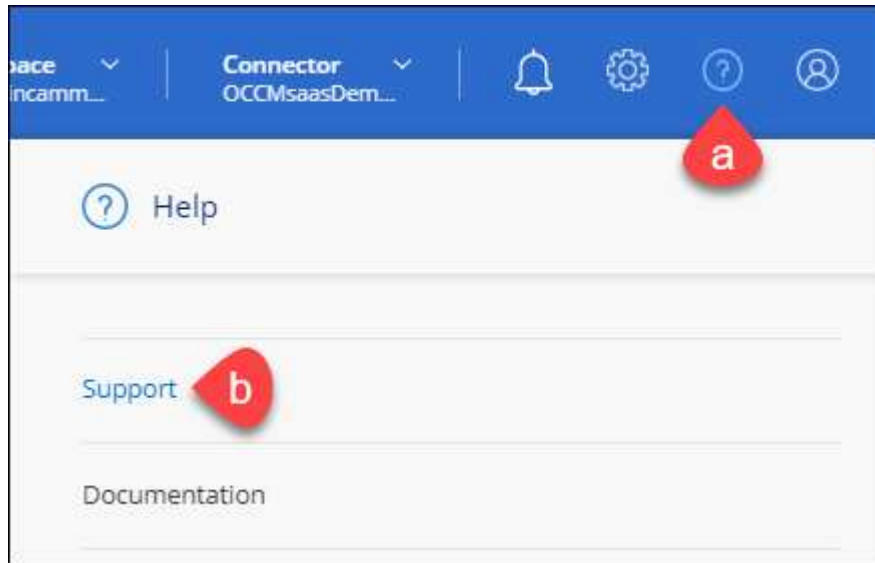
Agregue una cuenta NSS a BlueXP

La consola de soporte le permite añadir y gestionar sus cuentas de la página de soporte de NetApp para utilizarlas con 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 debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal).
- 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.

Regístrese en NetApp

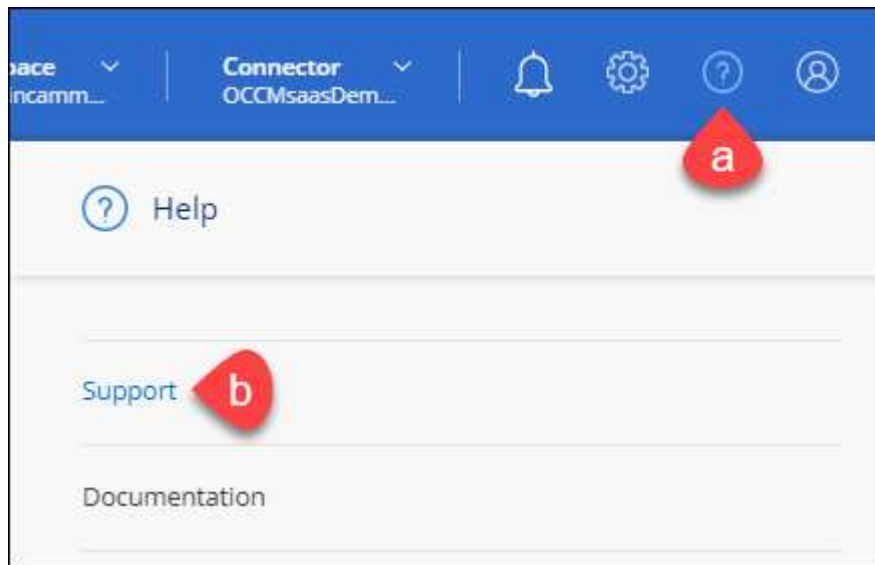
La forma de registrarse para recibir soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

Cliente existente con una cuenta de NSS

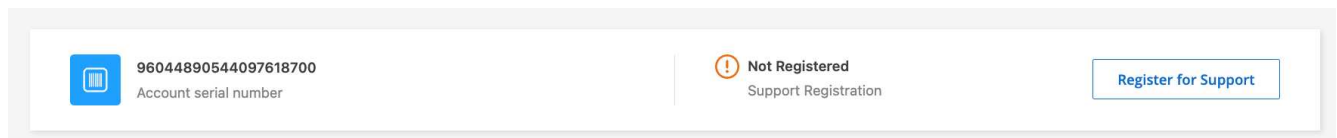
Si es cliente de NetApp con una cuenta de NSS, solo tiene que registrarse para recibir soporte a través de BlueXP.

Pasos

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



2. Si aún no lo ha hecho, agregue su cuenta NSS a BlueXP.
3. En la página **Recursos**, haga clic en **Registrar para asistencia**.



Cliente existente pero no cuenta NSS

Si ya es cliente de NetApp con licencias y números de serie existentes pero *no* cuenta de NSS, solo tiene que crear una cuenta de NSS.

Pasos

1. Complete el para crear una cuenta en la página de soporte de NetApp "[Formulario de registro de usuarios del sitio de soporte de NetApp](#)"
 - a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
 - b. Asegúrese de copiar el número de serie de la cuenta BlueXP (960xxxx) utilizado anteriormente para el

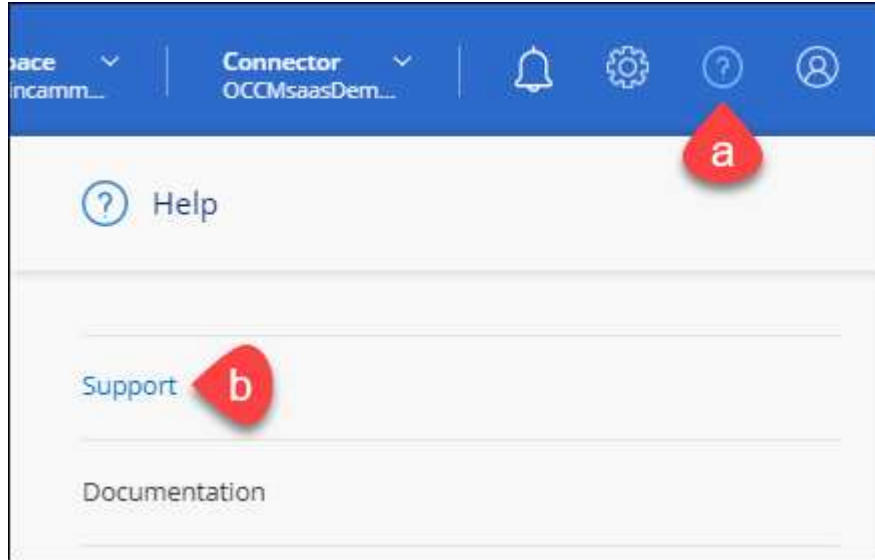
campo de número de serie. Esto agilizará el procesamiento de la cuenta.

Totalmente nuevo en NetApp

Si es totalmente nuevo en NetApp y no tiene una cuenta de NSS, siga cada paso que se indica a continuación.

Pasos

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



2. Busque el número de serie de su ID de cuenta en la página Support Registration.



3. Vaya a. "[Sitio de registro de soporte de NetApp](#)" Y seleccione **no soy un cliente registrado de NetApp**.
4. Rellene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **línea de productos**, seleccione **Cloud Manager** y, a continuación, seleccione el proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta desde el paso 2 anterior, complete la comprobación de seguridad y confirme que ha leído la Política de privacidad de datos global de NetApp.

Se envía inmediatamente un correo electrónico al buzón de correo para finalizar esta transacción segura. Asegúrese de comprobar sus carpetas de spam si el correo electrónico de validación no llega en pocos minutos.

7. Confirme la acción desde el correo electrónico.

Confirmar envía su solicitud a NetApp y recomienda que cree una cuenta en la página de soporte de NetApp.

8. Complete el para crear una cuenta en la página de soporte de NetApp "[Formulario de registro de usuarios del sitio de soporte de NetApp](#)"
 - a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de**

NetApp.

- b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.

Después de terminar

NetApp debería ponerse en contacto con usted durante este proceso. Este es un ejercicio de incorporación puntual para nuevos usuarios.

Una vez que tenga su cuenta de la página de soporte de NetApp, podrá navegar a BlueXP para añadir esta cuenta de NSS para futuros registros.

Obtenga ayuda

NetApp ofrece soporte para BlueXP y sus servicios cloud de diversas maneras. Hay disponibles amplias opciones de auto soporte gratuito las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimiento (KB) y un foro de la comunidad. Su registro de soporte incluye soporte técnico remoto a través de tickets web.

Autoasistencia

Estas opciones están disponibles de forma gratuita, las 24 horas del día, los 7 días de la semana:

- ["Base de conocimientos"](#)

Busque en la base de conocimientos de BlueXP para encontrar artículos útiles para resolver problemas.

- ["Comunidades"](#)

Únase a la comunidad de BlueXP para seguir los debates en curso o crear otros nuevos.

- Documentación

La documentación de BlueXP que está viendo actualmente.

- Correo: ng-cloudmanager-feedback@netapp.com [correo electrónico de comentarios]

Apreciamos sus opiniones. Envíe sus comentarios para ayudarnos a mejorar BlueXP.

Soporte de NetApp

Además de las opciones de autosoporte anteriores, puede trabajar con un especialista de soporte de NetApp para resolver cualquier problema después de activar el soporte de.

Antes de empezar

Para utilizar la capacidad **Crear un caso**, primero debe realizar un registro único del número de serie de su ID de cuenta de BlueXP (p. ej. 960xxxx) con NetApp. ["Aprenda a registrarse para obtener soporte"](#).

Pasos

1. En BlueXP, haga clic en **Ayuda > Soporte**.
2. Seleccione una de las opciones disponibles en Soporte técnico:
 - a. Haga clic en **Llame a nosotros** si desea hablar con alguien en el teléfono. Se le dirigirá a una página de netapp.com que enumera los números de teléfono a los que puede llamar.

b. Haga clic en **Crear un caso** para abrir una incidencia con los especialistas de soporte de NetApp:

- **Cuenta del sitio de soporte de NetApp:** Seleccione la cuenta de NSS correspondiente asociada con la persona que abre el caso de soporte. Esta persona será el contacto principal con NetApp para contactar con ella, además de los correos electrónicos adicionales que se proporcionan a continuación.

Si no ve su cuenta NSS, puede ir a la pestaña **NSS Management** de la sección Soporte de BlueXP para agregarla allí.

- **Servicio:** Seleccione el servicio con el que está asociado el problema. Por ejemplo, cuando BlueXP es específico de un problema de soporte técnico con flujos de trabajo o funcionalidades dentro del servicio.
- **Entorno de trabajo:** Si se aplica al almacenamiento, seleccione **Cloud Volumes ONTAP** o **On-Prem** y, a continuación, el entorno de trabajo asociado.


La lista de entornos de trabajo se encuentra dentro del ámbito de la cuenta BlueXP, el área de trabajo y el conector que ha seleccionado en el banner superior del servicio.

- **Prioridad de caso:** Elija la prioridad para el caso, que puede ser Baja, Media, Alta o crítica.

Para obtener más información sobre estas prioridades, pase el ratón sobre el icono de información situado junto al nombre del campo.


- **Descripción del problema:** Proporcione una descripción detallada del problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que haya realizado.
- **Direcciones de correo electrónico adicionales:** Introduzca direcciones de correo electrónico adicionales si desea que alguien más conozca este problema.

Create a Case


TESTCLOUD2NTAP 


NetApp Support Site Account


Service

Cloud Manager 

Working Environment


Select... 

Case Priority 


Low- General Guidance 

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) 

Attachment (Optional) Coming Soon

No files selected 

Después de terminar

Aparecerá una ventana emergente con el número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y le pondrá en contacto con usted próximamente.

Para obtener un historial de sus casos de soporte, puede hacer clic en **Configuración > línea de tiempo** y buscar acciones denominadas "Crear caso de soporte". Un botón situado en el extremo derecho le permite ampliar la acción para ver los detalles.

Es posible que se encuentre el siguiente mensaje de error al intentar crear un caso:

"No está autorizado a crear un caso en el servicio seleccionado"

Este error podría significar que la cuenta NSS y la compañía de registro con la que está asociada no es la

misma compañía de registro para el número de serie de la cuenta de BlueXP (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede consultar su lista de cuentas NSS en la parte superior del formulario **Crear un caso** para encontrar la coincidencia correcta, o puede buscar ayuda mediante una de las siguientes opciones:

- Usar el chat en el producto
- Envíe un caso no técnico en <https://mysupport.netapp.com/site/help>

Avisos legales

Los avisos legales proporcionan acceso a las declaraciones de copyright, marcas comerciales, patentes y mucho más.

Derechos de autor

<http://www.netapp.com/us/legal/copyright.aspx>

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Los demás nombres de empresas y productos son marcas comerciales de sus respectivos propietarios.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

Estadounidenses

Puede encontrar una lista actual de las patentes propiedad de NetApp en:

<https://www.netapp.com/us/media/patents-page.pdf>

Política de privacidad

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

Código abierto

Los archivos de notificación proporcionan información sobre los derechos de autor y las licencias de terceros que se utilizan en software de NetApp.

- ["Aviso para BlueXP"](#)

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.