Documentación de configuración y administración de BlueXP

Setup and administration

NetApp
April 24, 2024

Tabla de contenidos

Documentación de configuración y administración de BlueXP

Notas de la versión

Lo nuevo

Descubra las novedades de las funciones de administración de BlueXP: Cuentas BlueXP, conectores, credenciales de proveedores de nube y mucho más.

22 de abril de 2024

Conector 3.9.39

Esta versión de BlueXP Connector incluye mejoras de seguridad y correcciones de errores menores.

En este momento, la versión 3.9.39 está disponible para modo estándar y modo restringido.

Permisos de AWS para crear un conector

Ahora se necesitan dos permisos adicionales para crear un conector en AWS desde BlueXP:

```
"ec2:DescribeLaunchTemplates",
"ec2:CreateLaunchTemplate",
```

Estos permisos son necesarios para habilitar IMDSv2 en la instancia EC2 para el conector.

Hemos incluido estos permisos en la política que se muestra en la interfaz de usuario de BlueXP al crear un Connector y en la misma política que se proporciona en la documentación.

> Esta directiva sólo contiene los permisos necesarios para iniciar la instancia de Connector en AWS desde BlueXP. No es la misma política que se asigna a la instancia de Connector.

"Aprenda a configurar permisos de AWS para crear un conector desde AWS".

11 de abril de 2024

Actualización de Docker Engine

Hemos actualizado los requisitos de Docker Engine para especificar la versión máxima admitida en el conector, que es 25,0.5. La versión mínima admitida sigue siendo la 19,3.1.

"Ver requisitos del host de Connector".

26 de marzo de 2024

Versión en modo privado (3,9.38)

Ya está disponible una nueva versión del modo privado para BlueXP. Esta versión incluye las siguientes versiones de los servicios de BlueXP que son compatibles con el modo privado.

Servicio	Versión incluida
Conector	3.9.38
Backup y recuperación	12 de marzo de 2024
Clasificación	4 de marzo de 2024
Gestión de Cloud Volumes ONTAP	8 de marzo de 2024
Cartera digital	30 de julio de 2023
Gestión de clústeres de ONTAP en las instalaciones	30 de julio de 2023
Replicación	18 de septiembre de 2022

Esta nueva versión está disponible para descargar desde el sitio de soporte de NetApp.

- "Aprende sobre el modo privado"
- "Descubre cómo empezar a utilizar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"

8 de marzo de 2024

Conector 3.9.38

En este momento, la versión 3.9.38 está disponible para modo estándar y modo restringido. Esta versión incluye compatibilidad con IMDSv2 en AWS y una actualización de permisos de AWS.

Compatibilidad con IMDSv2

BlueXP ahora es compatible con el servicio de metadatos de la instancia de Amazon EC2 versión 2 (IMDSv2) con la instancia de conector y con las instancias de Cloud Volumes ONTAP. IMDSv2 proporciona protección mejorada contra vulnerabilidades. Anteriormente, solo IMDSv1 era compatible.

"Obtenga más información sobre IMDSv2 en el blog de seguridad de AWS"

El servicio de metadatos de instancia (IMDS) se activa de la siguiente forma en las instancias EC2:

- Para nuevas puestas en marcha de Connector de BlueXP o mediante "Guiones Terraform", IMDSv2 está activado por defecto en la instancia EC2.
- Si inicia una nueva instancia de EC2 en AWS y, a continuación, instala manualmente el software Connector, también se habilita IMDSv2 de forma predeterminada.
- Si inicia Connector desde AWS Marketplace, IMDSv1 está habilitado de forma predeterminada. Puede configurar manualmente IMDSv2 en la instancia de EC2.
- Para los conectores existentes, IMDSv1 sigue siendo compatible, pero puede configurar manualmente IMDSv2 en la instancia EC2 si lo prefiere.
- Para Cloud Volumes ONTAP, IMDSv1 se habilita de forma predeterminada en las instancias nuevas y existentes. Puede configurar manualmente IMDSv2 en las instancias EC2 si lo prefiere.

"Aprenda a configurar IMDSv2 en instancias existentes".

Actualización de permisos de AWS

Hemos actualizado la política de Connector para AWS para incluir el permiso «EC2:DescribeAvailabilityZones». Este permiso es necesario para una próxima versión. Actualizaremos las notas de la versión con más detalles cuando esa versión esté disponible.

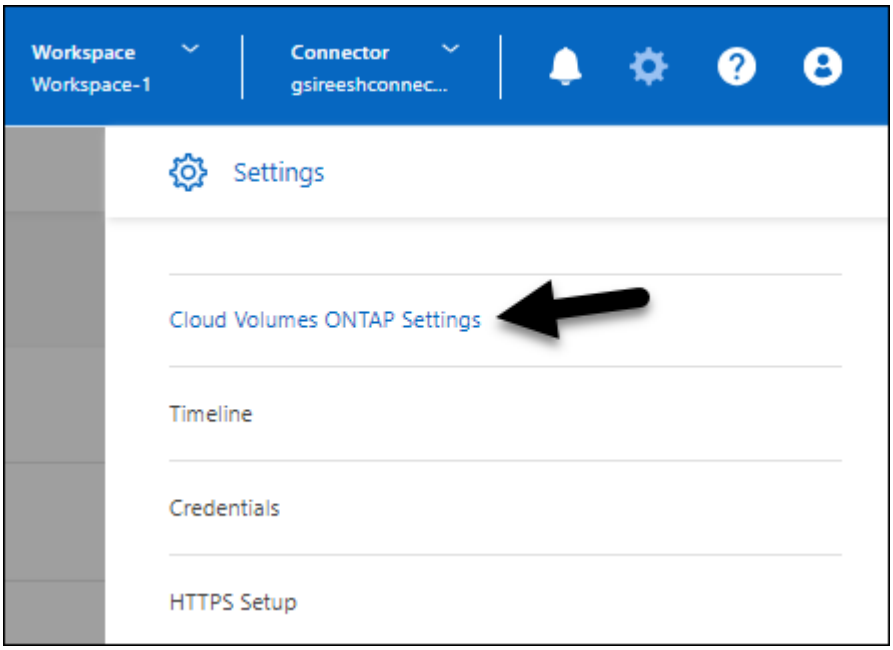
"Ver los permisos de AWS para el conector".

Configuración de proxy y configuración de Cloud Volumes ONTAP

La configuración del servidor proxy para el conector ahora está disponible en la página **Administrar conectores** (modo estándar) o en la página **Editar conectores** (modo restringido y modo privado).

"Aprenda a configurar Connector para usar un servidor proxy".

Además, cambiamos el nombre de la página **Configuración del conector** a **Configuración de Cloud Volumes ONTAP**.



15 de febrero de 2024

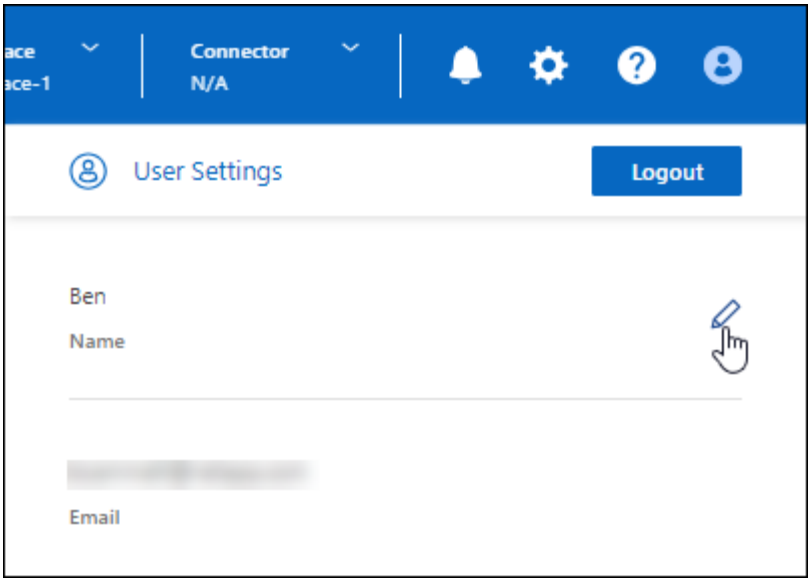
Conector 3.9.37

Esta versión de BlueXP Connector incluye mejoras de seguridad y correcciones de errores menores.

En este momento, la versión 3.9.37 está disponible para modo estándar y modo restringido.

Editar nombre

Si usas las credenciales de la nube de NetApp para iniciar sesión en BlueXP, ahora puedes editar tu nombre en **Configuración de usuario**.



No se puede editar su nombre si inicia sesión con una conexión federada o con su cuenta del sitio de soporte de NetApp.

11 de enero de 2024

Conector 3.9.36

Esta versión incluye mejoras menores, correcciones de errores y soporte para Connector en las siguientes regiones de nube:

- La región de Israel (Tel Aviv) en AWS
- La región de Arabia Saudita en Google Cloud

5 de diciembre de 2023

Versión en modo privado (3,9.35)

Ya está disponible una nueva versión del modo privado para BlueXP. Esta versión incluye la versión 3.9.35 del conector y versiones de los servicios de BlueXP compatibles con el modo privado a partir de octubre de 2023.

Esta nueva versión está disponible para descargar desde el sitio de soporte de NetApp.

- "Obtén más información sobre los servicios de BlueXP que se incluyen en el modo privado"
- "Descubre cómo empezar a utilizar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"

8 de noviembre de 2023

Conector 3.9.35

Esta versión incluye mejoras de seguridad y correcciones de errores menores.

6 de octubre de 2023

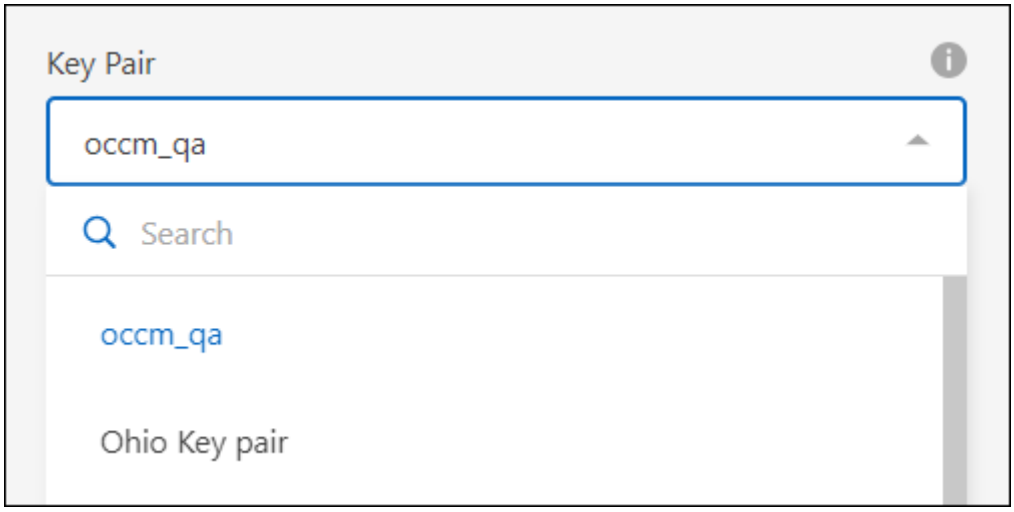
Conector 3.9.34

Esta versión incluye mejoras y correcciones de errores menores.

10 de septiembre de 2023

Conector 3.9.33

- Cuando creas un conector en AWS desde BlueXP, ahora puedes buscar dentro del campo Par de claves para encontrar más fácilmente el par de claves que quieres usar con la instancia de Connector.



- Esta actualización también incluye correcciones de errores.

30 de julio de 2023

Conector 3.9.32

- Ahora puedes usar la API del servicio de auditoría de BlueXP para exportar registros de auditoría.

  El servicio de auditoría registra información sobre las operaciones realizadas por los servicios de BlueXP. Esto incluye espacios de trabajo, conectores utilizados y otros datos de telemetría. Puede utilizar estos datos para determinar qué acciones se realizaron, quién las realizó y cuándo ocurrieron.

  "Obtenga más información sobre el uso de la API del servicio de auditoría"

  Tenga en cuenta que también se puede acceder a este enlace desde la interfaz de usuario de BlueXP en la página Timeline.

- 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"

2 de julio de 2023

Conector 3.9.31

- Ahora puede descubrir clústeres de ONTAP en las instalaciones desde la pestaña **Mi estado** (anteriormente **Mis oportunidades**)

  "Aprenda a descubrir clústeres en la página Mi estado".

- Si utiliza el conector en una región de gobierno de Azure, debe asegurarse de que el conector puede ponerse en contacto con el siguiente punto final:

  https://occmclientinfragov.azurecr.us

  Este punto final es necesario para instalar manualmente el conector y para actualizar el conector y sus componentes Docker.

  Como resultado de este cambio, un conector en una región de Azure Government ya no contacta con el siguiente punto final:

  https://cloudmanagerinfraprod.azurecr.io

  Tenga en cuenta que este punto final sigue siendo necesario para todas las demás configuraciones de modo restringido y para el modo estándar.

4 de junio de 2023

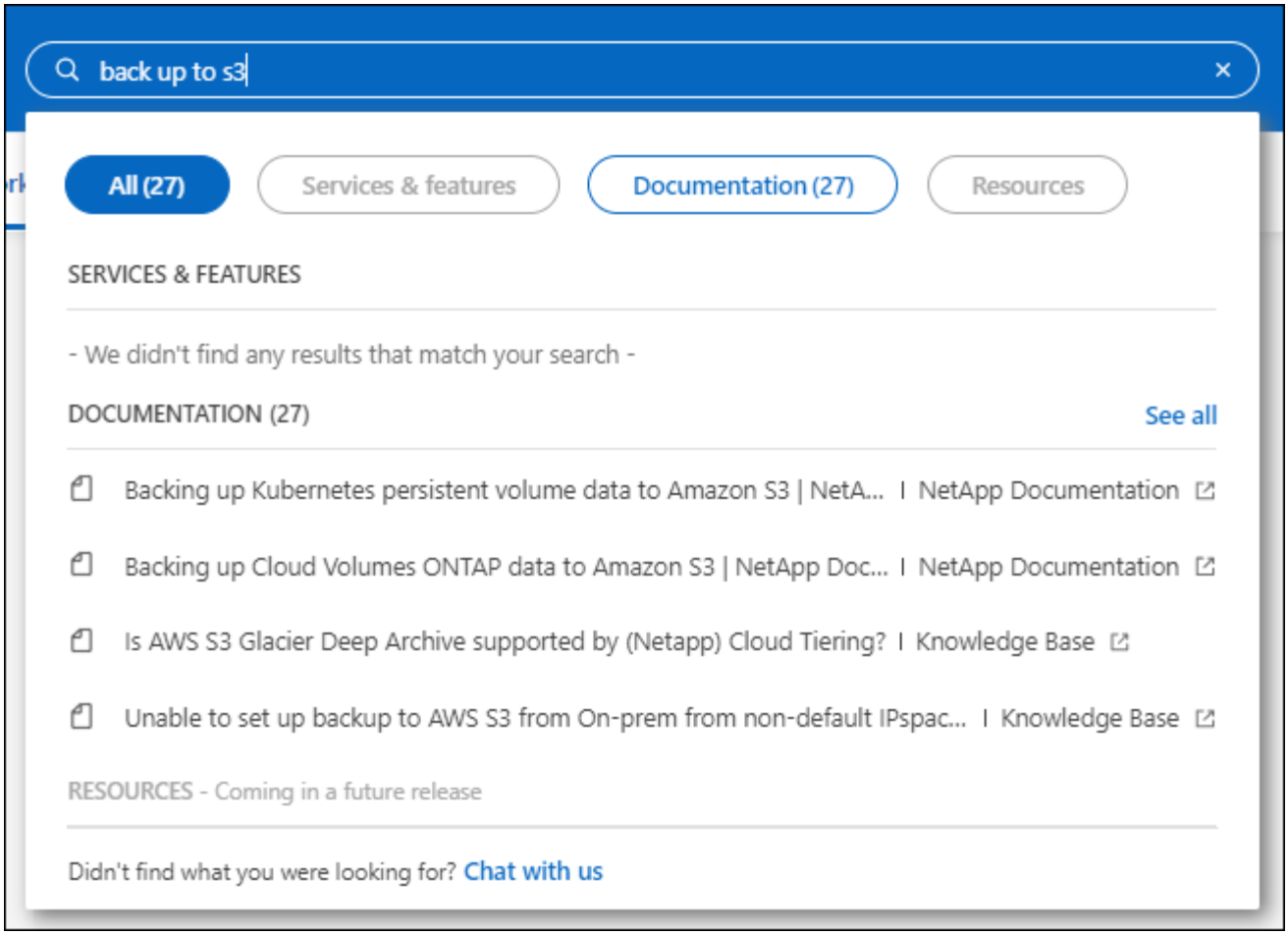
Conector 3.9.30

- Al abrir un caso de soporte de NetApp desde la consola de soporte, BlueXP ahora abre el caso con la cuenta del sitio de soporte de NetApp asociada con tu inicio de sesión en BlueXP. BlueXP ya usaba la cuenta del sitio de soporte de NetApp asociada con toda la cuenta de BlueXP.

  Como parte de este cambio, el registro de soporte para una cuenta de BlueXP se realiza a través de la cuenta del sitio de soporte de NetApp asociada con el inicio de sesión de un usuario en BlueXP. Anteriormente, el registro de soporte se realizaba a través de una cuenta NSS asociada a toda la cuenta de BlueXP. Como resultado, los demás usuarios de BlueXP no verán el mismo estado de registro de soporte si no han asociado una cuenta de sitio de soporte de NetApp con su inicio de sesión de BlueXP. Si has registrado anteriormente tu cuenta de BlueXP para soporte, el estado de registro sigue siendo válido. Solo necesita agregar una cuenta NSS a nivel de usuario para ver el estado.

  - "Aprenda a crear un caso con el soporte de NetApp"
  - "Descubre cómo gestionar las credenciales asociadas con tu inicio de sesión de BlueXP"
  - "Aprenda a registrarse para obtener soporte"

- Ahora puedes buscar la documentación en BlueXP. Los resultados de búsqueda ahora proporcionan enlaces a contenido en docs.netapp.com y kb.netapp.com, lo que podría ayudar a responder una pregunta que tenga.



- Ahora, Connector te permite añadir y gestionar cuentas de almacenamiento de Azure desde BlueXP.

  "Descubre cómo añadir nuevas cuentas de almacenamiento de Azure a tus suscripciones de Azure desde BlueXP".

- El conector ahora es compatible con las siguientes regiones de AWS:
  - Hyderabad (ap-SUR-2)
  - Melbourne (ap-sureste-4)
  - España (eu-SUR-2)
  - EAU (ME-CENTRAL-1)
  - Zúrich (eu-CENTRAL-2)
- El conector ahora es compatible con las siguientes regiones de Azure:
  - Brasil Sur
  - Francia Sur
  - Jio India Central
  - Jio India West
  - Polonia Central
  - Qatar Central
- Ahora el conector es compatible con las siguientes regiones de Google Cloud:

- Colón (EE. UU.-este 5)
- Dallas (EE.UU.-sur-1)

"Consulte la lista completa de las regiones admitidas"

7 de mayo de 2023

Conector 3.9.29

- Ubuntu 22,04 es el nuevo sistema operativo para Connector cuando se pone en marcha un Connector desde BlueXP o desde el mercado de tu proveedor de nube.

  También tiene la opción de instalar manualmente el conector en su propio host Linux que ejecuta Ubuntu 22,04.

- Red Hat Enterprise Linux 8,6 y 8,7 ya no son compatibles con las nuevas implementaciones de Connector.

  Estas versiones no son compatibles con nuevas implementaciones porque Red Hat ya no es compatible con Docker, que es necesario para Connector. Si tiene un conector existente ejecutándose en RHEL 8,6 o 8,7, NetApp seguirá admitiendo su configuración.

  Red Hat 7,6, 7,7, 7,8 y 7,9 siguen siendo compatibles con conectores nuevos y existentes.

- El conector ahora es compatible en la región de Qatar en Google Cloud.
- El conector también es compatible con la región central de Suecia en Microsoft Azure.

  "Consulte la lista completa de las regiones admitidas"

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

  "Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"

4 de abril de 2023

Modos de implementación

BlueXP *modos de implementación* le permiten utilizar BlueXP de forma que se ajuste a sus requisitos empresariales y de seguridad. Puede elegir entre tres modos:

- Modo estándar
- Modo restringido
- Modo privado

"Obtenga más información sobre estos modos de implementación".

> La introducción del modo restringido sustituye a la opción de activar o desactivar la plataforma SaaS. Puede habilitar el modo restringido en el momento de crear una cuenta. No se puede habilitar ni deshabilitar más adelante.

3 de abril de 2023

Conector 3.9.28

- Las notificaciones por correo electrónico ahora son compatibles con la cartera digital de BlueXP.

  Si configura los ajustes de notificación, puede recibir notificaciones por correo electrónico cuando sus licencias de BYOL estén a punto de expirar (una notificación de "advertencia") o si ya han caducado (una notificación de "error").

  "Aprenda a configurar notificaciones por correo electrónico".

- El conector ahora es compatible con la región de Google Cloud en Turín.

  "Consulte la lista completa de las regiones admitidas"

- Ahora puede gestionar las credenciales de usuario asociadas con su inicio de sesión de BlueXP: Credenciales de ONTAP y credenciales del sitio de soporte de NetApp (NSS).

  Al ir a **Configuración > credenciales**, puede ver las credenciales, actualizar las credenciales y eliminarlas. Por ejemplo, si cambia la contraseña para estas credenciales, deberá actualizar la contraseña en BlueXP.

  "Aprenda a gestionar las credenciales de usuario".

- Ahora puede cargar archivos adjuntos al crear un caso de soporte o al actualizar las notas del caso para un caso de soporte existente.

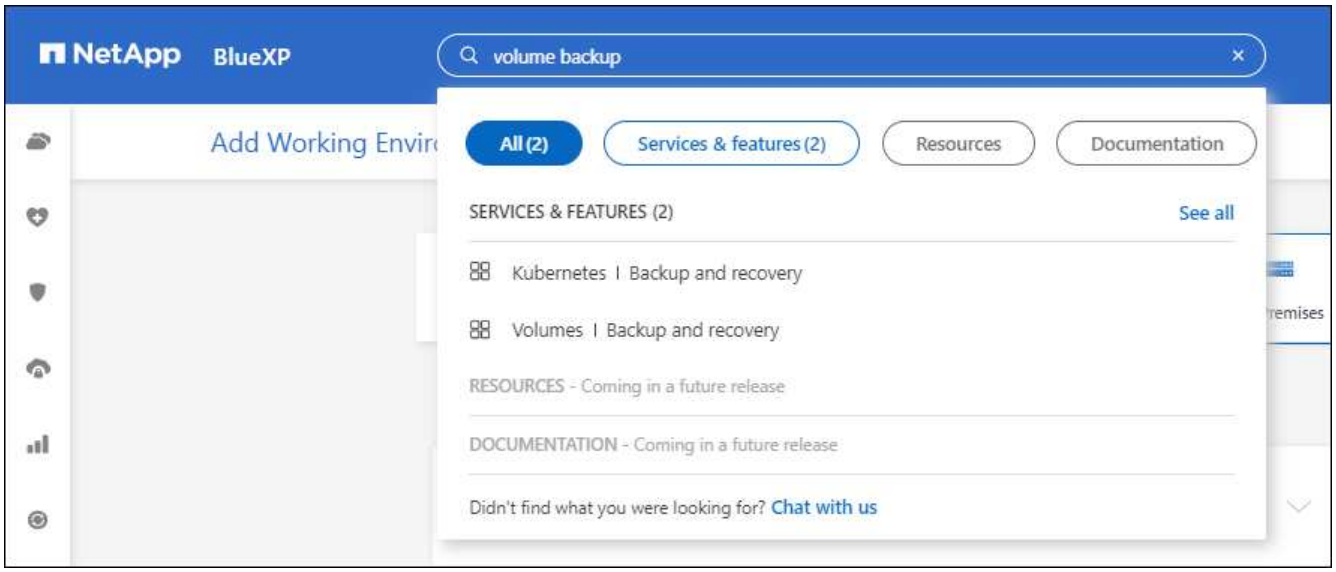
  "Descubra cómo crear y gestionar casos de soporte".

- 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"

5 de marzo de 2023

Conector 3.9.27

- La búsqueda ya está disponible en la consola BlueXP. En este momento, puede utilizar la búsqueda para buscar servicios y características de BlueXP.



- Puede ver y gestionar los casos de soporte activos y resueltos directamente desde BlueXP. Es posible gestionar los casos asociados con su cuenta de NSS y con su empresa.

  "Aprenda a gestionar sus casos de soporte".

- El conector ahora es compatible con cualquier entorno de nube que tenga un aislamiento completo de Internet. A continuación, puede usar la consola BlueXP que se ejecuta en el conector para implementar Cloud Volumes ONTAP en la misma ubicación y detectar clústeres de ONTAP en las instalaciones (si tiene una conexión desde su entorno de cloud a un entorno local). También puedes utilizar el backup y la recuperación de datos de BlueXP para realizar backups de volúmenes de Cloud Volumes ONTAP en las regiones comerciales de AWS y Azure. No hay otros servicios de BlueXP compatibles con este tipo de puesta en marcha, a excepción de la cartera digital de BlueXP.

  La región de la nube puede ser una región para agencias estadounidenses seguras como AWS Top Secret Cloud, AWS Secret Cloud, Azure IL6 o cualquier región comercial.

  Para empezar, instale manualmente el software Connector, inicie sesión en la consola BlueXP que se ejecuta en el conector, añada la licencia BYOL a la cartera digital de BlueXP y, después, implemente Cloud Volumes ONTAP.

  - "Instale el conector en una ubicación sin acceso a Internet"
  - "Acceda a la consola BlueXP del conector"
  - "Añada una licencia sin asignar"
  - "Empiece a usar Cloud Volumes ONTAP"

- El conector ahora le permite agregar y gestionar cubos de Amazon S3 desde BlueXP.

  "Vea cómo añadir nuevos bloques de Amazon S3 en su cuenta de AWS desde BlueXP".

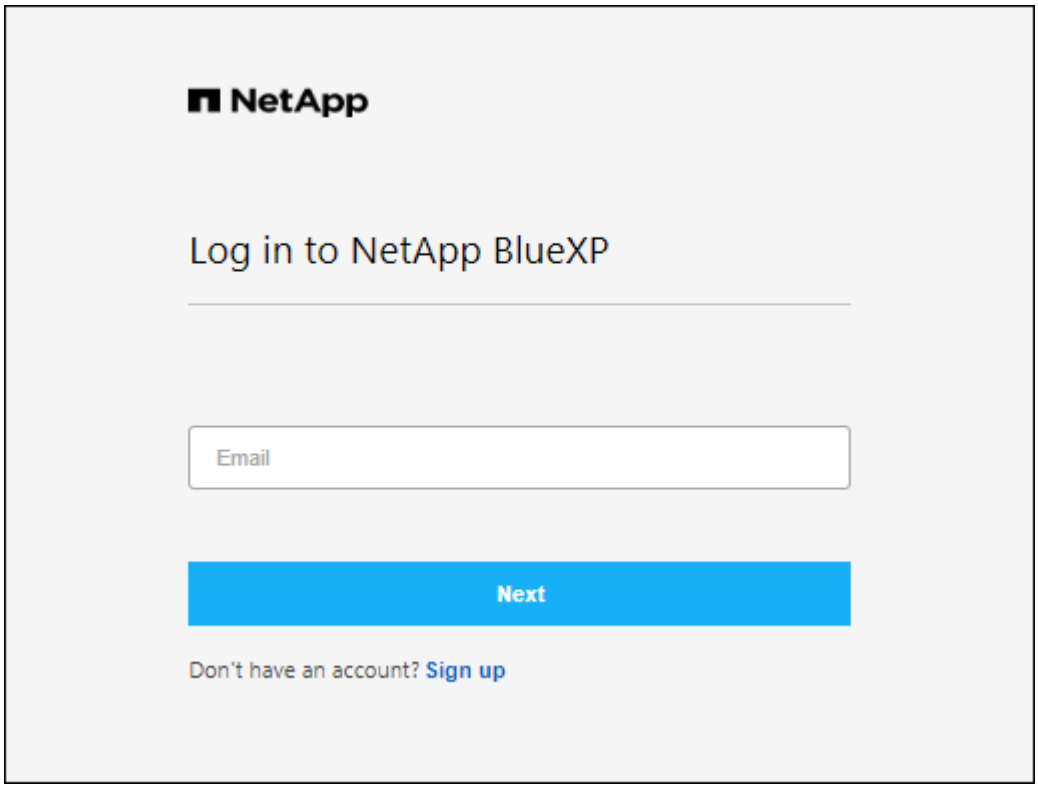
- Esta versión del conector incluye mejoras de Cloud Volumes ONTAP.

  "Obtenga información acerca de las mejoras de Cloud Volumes ONTAP"

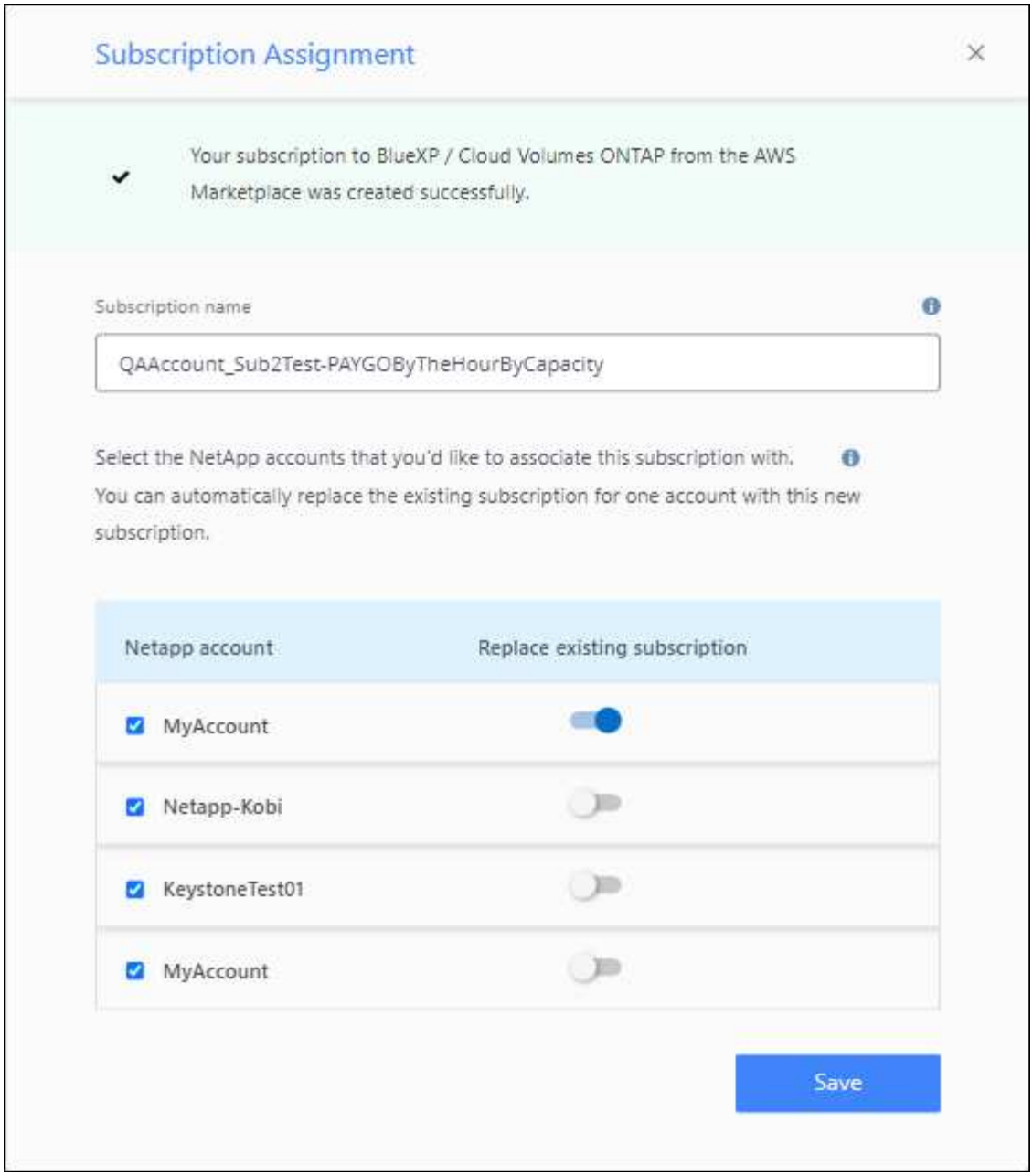
5 de febrero de 2023

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 seleccionar **Siguiente**, BlueXP te pide que te autentiques mediante el método de autenticación asociado con tu 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.



  - "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

- Ya puedes ver y gestionar tus suscripciones PAYGO y los contratos anuales de BlueXP desde la cartera digital.

  "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

Introducción de BlueXP

NetApp BlueXP amplía y mejora las funcionalidades que se proporcionan a través de Cloud Manager. BlueXP es un plano de control unificado que proporciona una experiencia multicloud híbrida para servicios de almacenamiento y datos en los entornos de almacenamiento y de cloud en las instalaciones.

Experiencia de gestión unificada

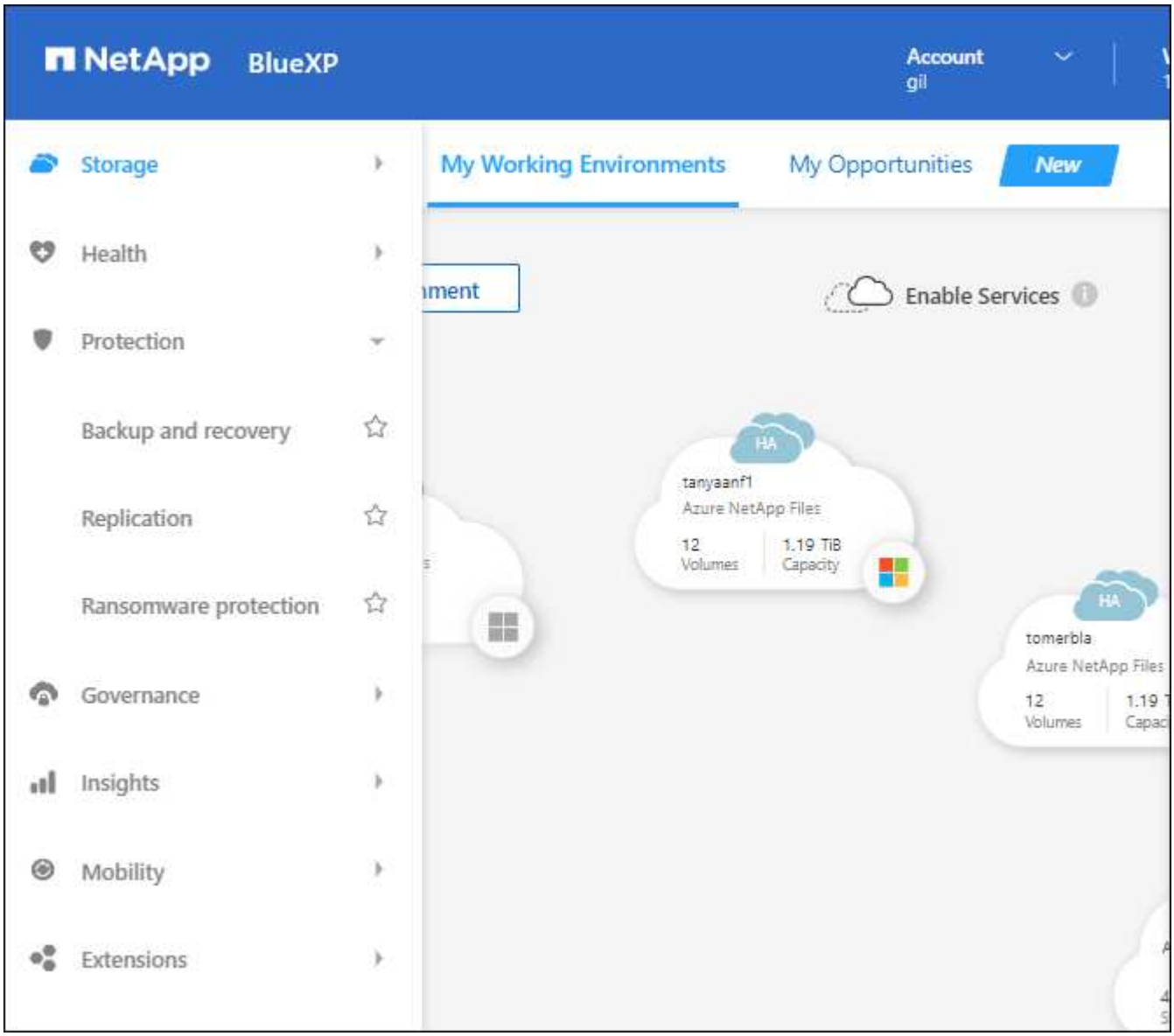
BlueXP le permite gestionar todos sus activos de almacenamiento y datos desde una única interfaz.

Puedes usar BlueXP para crear y administrar almacenamiento en nube (por ejemplo, Cloud Volumes ONTAP y Azure NetApp Files), para mover, proteger y analizar datos, y para controlar muchos dispositivos de almacenamiento on-premises y en la periferia.

"Obtenga más información en el sitio Web de BlueXP"

Nuevo menú de navegación

En el menú de navegación de BlueXP, los servicios ahora están organizados por categorías y se denominan según su funcionalidad. Por ejemplo, puedes acceder a la copia de seguridad y recuperación de BlueXP desde la categoría **Protección**.



Integraciones de nuevos productos

- Ahora puede gestionar los bloques de Amazon S3 en las cuentas de AWS donde está instalado Connector.
- Ahora puede gestionar más sistemas de almacenamiento en las instalaciones, como E-Series y StorageGRID.
- Ahora puedes utilizar servicios de datos que antes solo estaban disponibles como servicio independiente con una interfaz de usuario independiente, como el asesor digital de BlueXP (Active IQ).

Leer más

- "Gestión de bloques de Amazon S3"

- "Gestione los sistemas de almacenamiento E-Series"
- "Gestione los sistemas de almacenamiento StorageGRID"
- "Obtenga información sobre la integración de Digital Advisor"

Solicitar que se actualicen las credenciales de NSS

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.

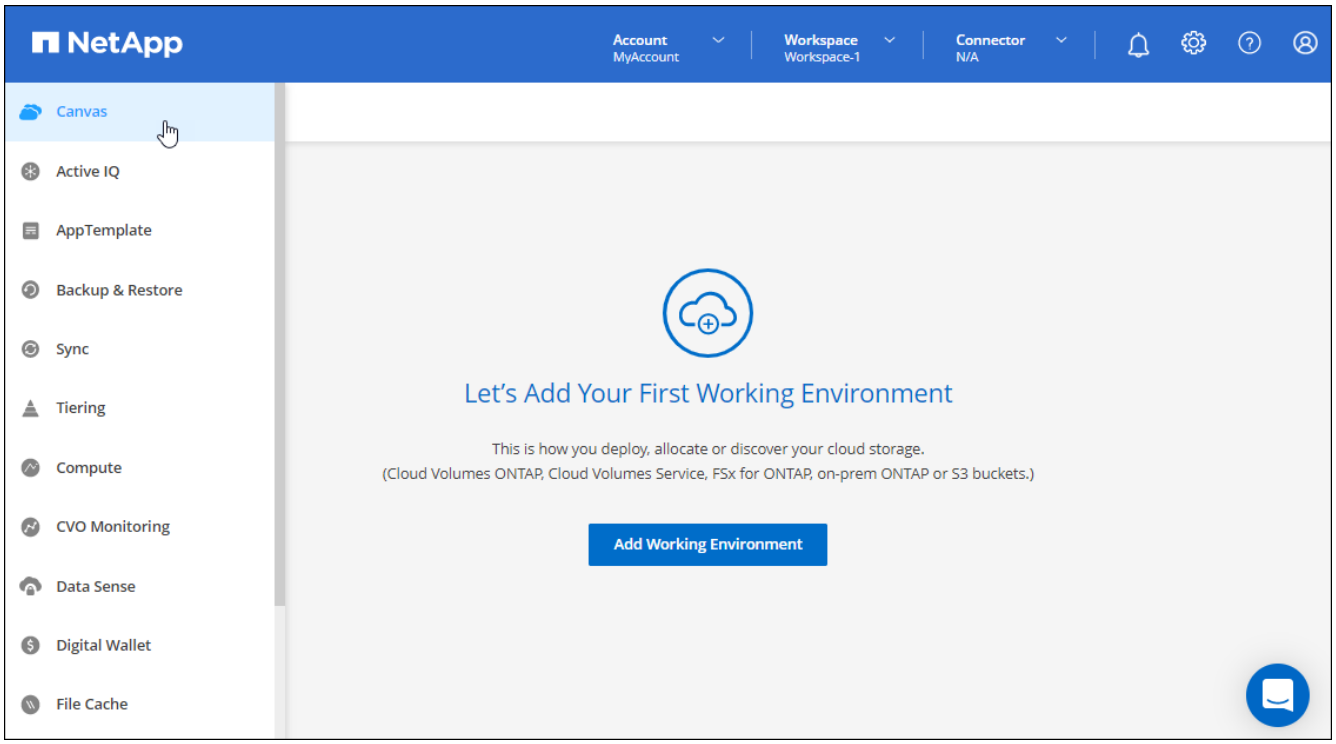
"A continuación se muestra un ejemplo en el que se muestran los permisos de la función IAM de AWS que se utilizan para crear un conector".

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.



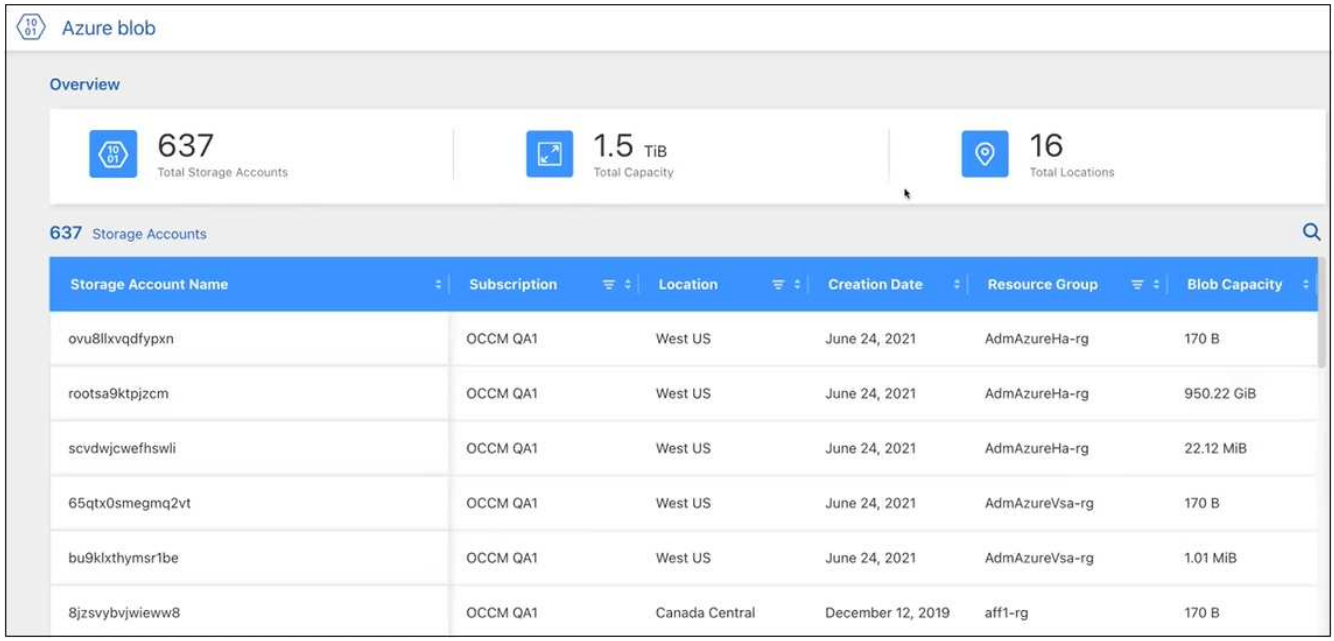
- Ahora puede configurar Cloud Manager para que envíe notificaciones por correo electrónico, de modo que se le pueda informar de la actividad importante del sistema incluso si no ha iniciado sesión en el sistema.

  "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:



- 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.

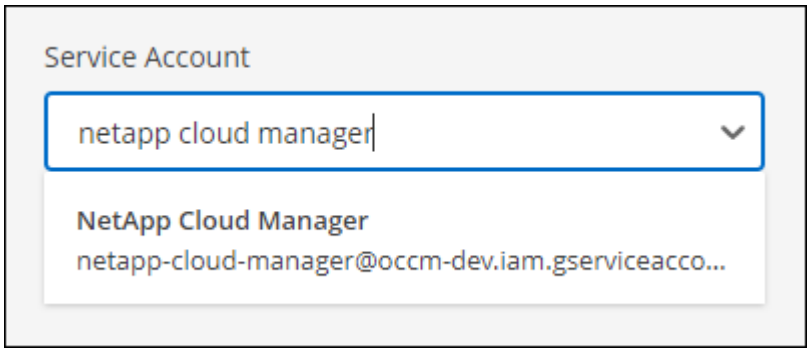
2 de mayo de 2022

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

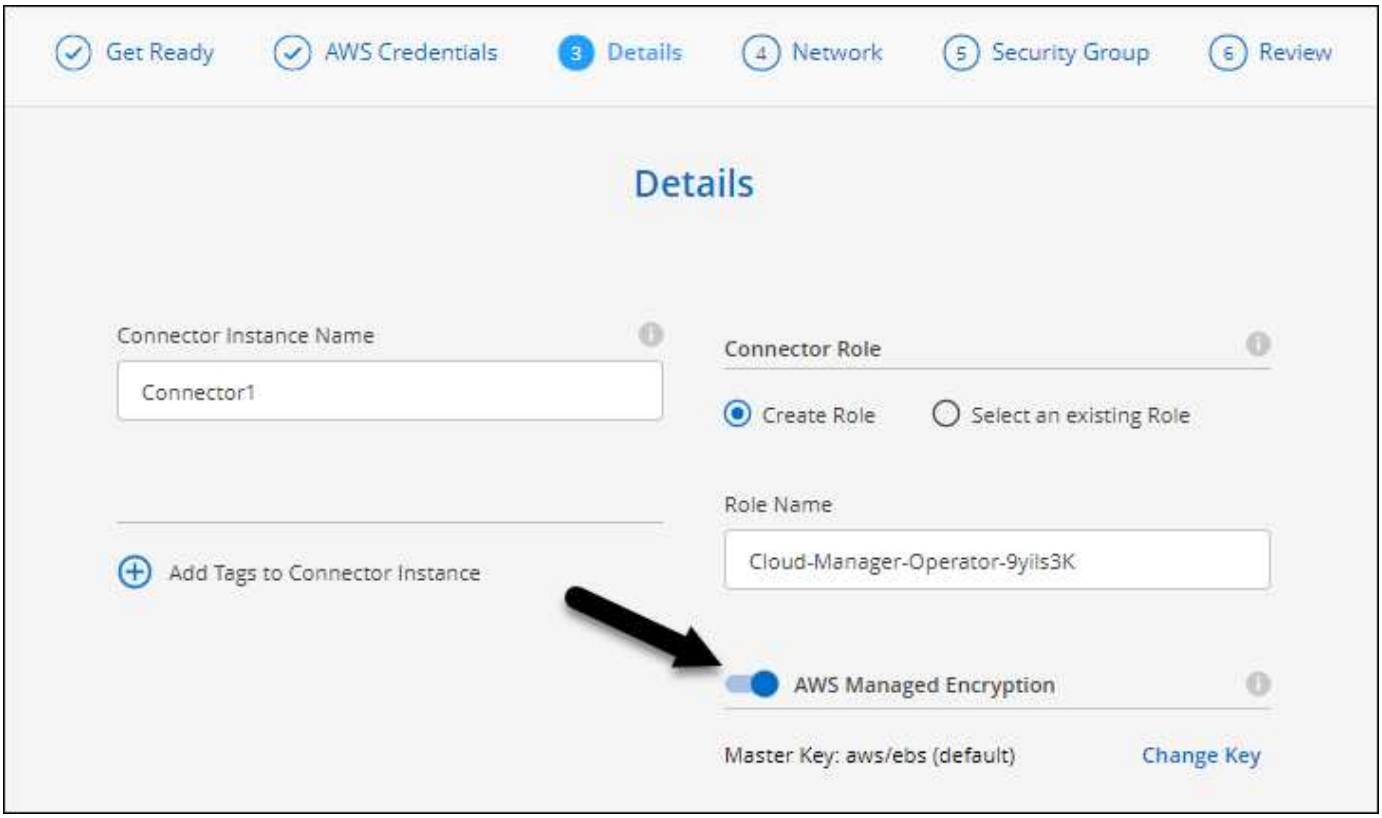
Puntos finales reducidos para el conector

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"

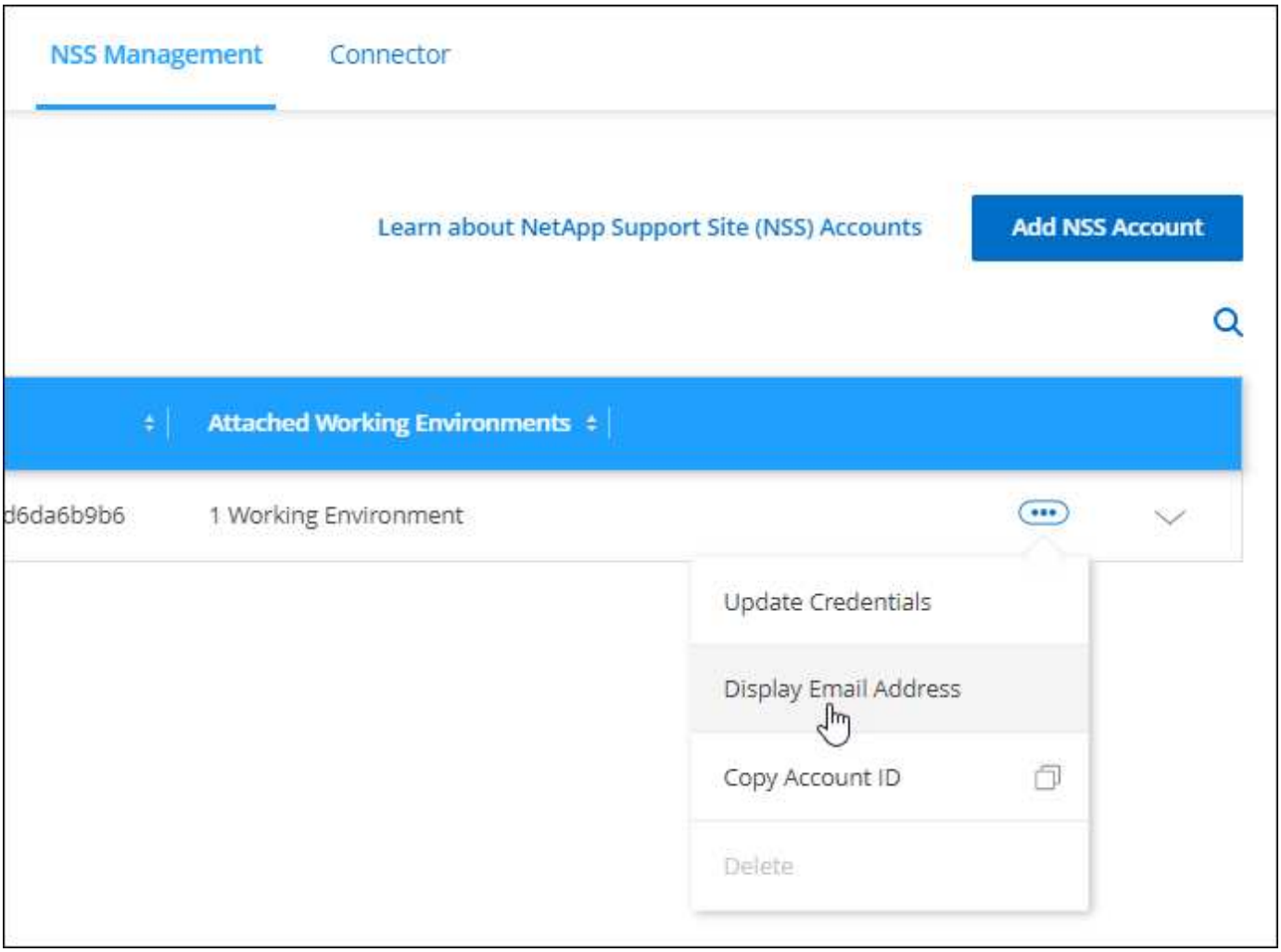
Cifrado de disco EBS para el conector

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.



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.

"Obtenga más información sobre el uso por parte de NetApp de Microsoft Azure Active Directory 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".

7 de julio de 2021

Mejoras en el asistente Agregar conector

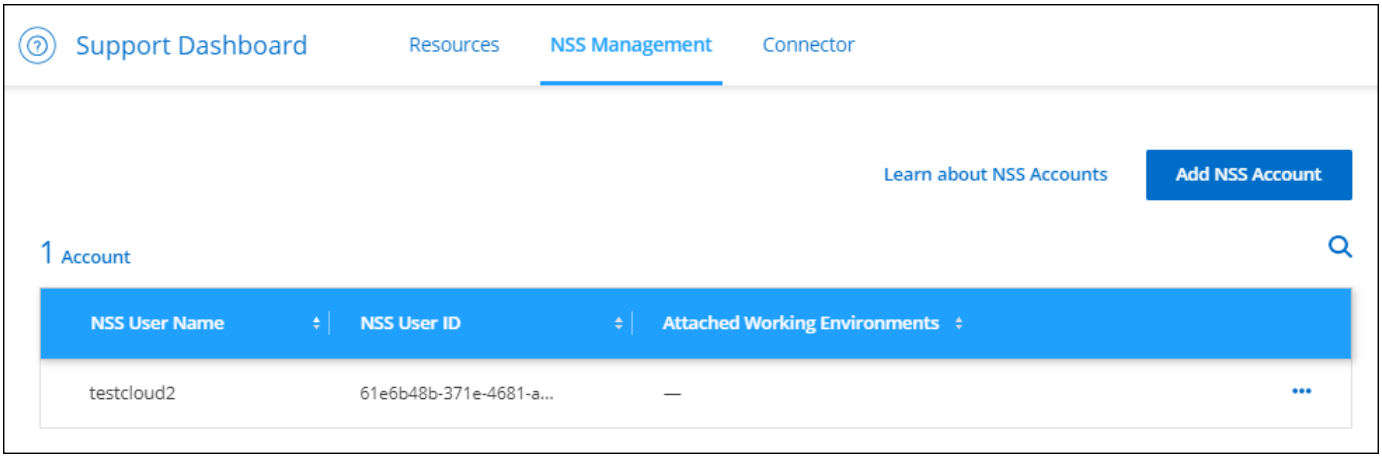
Hemos rediseñado el asistente **Add Connector** para añadir nuevas opciones y facilitar su uso. Ahora puede añadir etiquetas, especificar un rol (para AWS o Azure), cargar un certificado raíz para un servidor proxy, ver código para la automatización de Terraform, ver detalles del progreso, etc.

- "Cree un conector en AWS"
- "Cree un conector en Azure"
- "Cree un conector en Google Cloud"

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".

8 de marzo de 2021

Esta actualización incluye mejoras en varias características y servicios.

Mejoras de Cloud Volumes ONTAP

Esta versión de Cloud Manager incluye mejoras en la gestión de Cloud Volumes ONTAP.

Mejora disponible en todos los proveedores de cloud

Cloud Manager ahora puede poner en marcha y gestionar Cloud Volumes ONTAP 9,9.0.

"Conozca cuáles son las nuevas funciones que se incluyen en esta versión de Cloud Volumes ONTAP".

Mejoras disponibles en AWS

- Ahora puede implementar Cloud Volumes ONTAP 9.8 en el entorno de servicios de cloud comercial (C2S) de AWS.

  "Aprenda cómo empezar en C2S"

- Cloud Manager siempre le ha permitido cifrar datos de Cloud Volumes ONTAP mediante el servicio de gestión de claves (KMS) de AWS. A partir de Cloud Volumes ONTAP 9.9.0, los datos en discos EBS y los datos organizados en niveles en S3 se cifran si selecciona un CMK gestionado por el cliente. Anteriormente, solo se cifraban los datos de EBS.

  Tenga en cuenta que deberá proporcionar acceso a la función IAM de Cloud Volumes ONTAP para poder utilizar el CMK.

  "Más información sobre la configuración de AWS KMS con Cloud Volumes ONTAP"

Mejora disponible en Azure

Ahora puede implementar Cloud Volumes ONTAP 9.8 en el nivel de impacto 6 (IL6) del Departamento de Defensa de Azure (DoD).

Mejoras disponibles en Google Cloud

- Hemos reducido el número de direcciones IP necesarias para Cloud Volumes ONTAP 9.8 y versiones posteriores en Google Cloud. De forma predeterminada, se requiere una dirección IP menor (unificamos la LIF de interconexión de clústeres con la LIF de gestión de nodos). También tiene la opción de omitir la

creación de la LIF de gestión de SVM al usar la API, lo que reduciría la necesidad de usar una dirección IP adicional.

"Más información acerca de los requisitos de dirección IP en Google Cloud"

- Al poner en marcha un par de alta disponibilidad de Cloud Volumes ONTAP en Google Cloud, ahora puede elegir VPC compartidos para VPC-1, VPC-2 y VPC-3. Anteriormente, solo VPC-0 podía ser un VPC compartido. Este cambio es compatible con Cloud Volumes ONTAP 9.8 y versiones posteriores.

  "Obtenga más información acerca de los requisitos de red de Google Cloud"

Mejoras en los conectores

- Ahora Cloud Manager notifica a los usuarios administradores mediante un correo electrónico cuando no se está ejecutando un conector.

  Mantener sus conectores en funcionamiento ayuda a garantizar la mejor gestión de Cloud Volumes ONTAP y otros servicios en la nube de NetApp.

- Cloud Manager ahora muestra una notificación si necesita cambiar el tipo de instancia de su Connector.

  Al cambiar el tipo de instancia, se garantiza que puede utilizar las nuevas funciones y capacidades que le faltan actualmente.

Mejoras de Cloud Sync

- Cloud Sync ahora admite relaciones de sincronización entre el almacenamiento de ONTAP S3 y servidores SMB:
  - Almacenamiento de ONTAP S3 en un servidor SMB
  - Un servidor SMB para el almacenamiento S3 de ONTAP

    "Consulte las relaciones de sincronización compatibles"

- Cloud Sync ahora le permite unificar la configuración de un grupo de agentes de datos directamente desde la interfaz de usuario.

  No recomendamos cambiar la configuración por su cuenta. Debe consultar con NetApp para saber cuándo cambiar la configuración y cómo modificarla.

  "Obtenga más información sobre cómo definir una configuración unificada"

Mejoras en la organización en niveles del cloud

- Al organizar en niveles en Google Cloud Storage, puedes aplicar una regla de ciclo de vida, de modo que los datos organizados en niveles pasen de la clase de almacenamiento estándar al almacenamiento Nearline, Coldline o Archive de menor coste transcurridos 30 días.
- Ahora Cloud Tiering muestra si tienes clústeres de ONTAP en las instalaciones sin detectar de manera que puedas añadirlos a Cloud Manager para permitir la organización en niveles u otros servicios en esos clústeres.

  "Descubra cómo detectar estos clústeres adicionales"

Mejoras de Azure NetApp Files

Ahora puede cambiar de forma dinámica el nivel de servicio de un volumen para satisfacer las necesidades de las cargas de trabajo y optimizar los costes. El volumen se mueve al otro pool de capacidad sin afectar al volumen. "Leer más"

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

No se admiten servidores proxy transparentes

BlueXP no admite servidores proxy transparentes con el conector.

"Obtenga más información sobre el uso de un servidor proxy con Connector".

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 consola basada en web que se ejecuta en un conector, es posible que la interfaz no se muestre a veces y sólo 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.

Manos a la obra

Aprenda lo básico

Más información sobre BlueXP

NetApp BlueXP proporciona a su organización un plano de control único que le ayuda a crear, proteger y dirigir los datos tanto en sus instalaciones como en sus entornos de cloud. La plataforma SaaS de BlueXP incluye servicios que proporcionan gestión del almacenamiento, movilidad de datos, protección de datos, y análisis y control de los datos. Las capacidades de gestión se proporcionan a través de una consola basada en web y API.

Funciones

La plataforma BlueXP proporciona cuatro pilares principales de la gestión de datos: Almacenamiento, movilidad, protección, análisis y control.

Reducida

Descubra, ponga en marcha y gestione el almacenamiento, ya sea en AWS, Azure, Google Cloud o en las instalaciones.

- 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

Movilidad

Mueva los datos donde los necesite sincronizando, copiando, organizando en niveles y almacenando los datos en caché.

- "Copiar y sincronizar"
- "Almacenamiento en caché en el edge"
- "Organización en niveles"

Protección

Use mecanismos de protección automatizados para proteger los datos contra la pérdida de datos, interrupciones del servicio no planificadas, ransomware y otras amenazas cibernéticas.

- "Backup y recuperación"

- "Replicación"
- "Protección de datos para cargas de trabajo de Kubernetes"

Análisis y control

Use herramientas para supervisar, asignar y optimizar su almacenamiento de datos y su infraestructura. Obtenga información procesable para optimizar el estado, la resiliencia y la economía del almacenamiento.

- "Clasificación"
- "Asesor digital"
- "Eficiencia económica"
- "Resiliencia operativa"

"Obtenga más información sobre cómo puede utilizar BlueXP para ayudar a su organización"

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 consola basada en web que se proporciona a través de la capa de SaaS, cuentas que proporcionan multi-tenancy y conectores que gestionan los entornos de trabajo y habilitan los servicios en la nube de BlueXP.

Software como servicio

BlueXP es accesible a través de un "consola basada en web" Y API. Esta experiencia SaaS le permite acceder automáticamente a las últimas funciones a medida que se publican y cambiar fácilmente entre sus cuentas y conectores de BlueXP.

Cuenta BlueXP

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

"Más información acerca de las cuentas".

Conectores

No necesitas un conector para empezar con BlueXP, pero tendrás que crear un conector para desbloquear todas las funciones y servicios de BlueXP. Un conector permite la gestión de recursos y procesos en sus entornos locales y de cloud. Es necesario gestionar entornos de trabajo (por ejemplo, Cloud Volumes ONTAP y clústeres de ONTAP en las instalaciones) y usar muchos servicios de datos de BlueXP.

"Más información sobre conectores".

Modo restringido y modo privado

BlueXP también es compatible en entornos que tienen restricciones de seguridad y conectividad. Puede utilizar *restricted mode* o *private mode* para limitar la conectividad saliente a la capa SaaS BlueXP.

"Obtenga más información sobre los modos de implementación de BlueXP".

Certificación SOC 2 de tipo 2

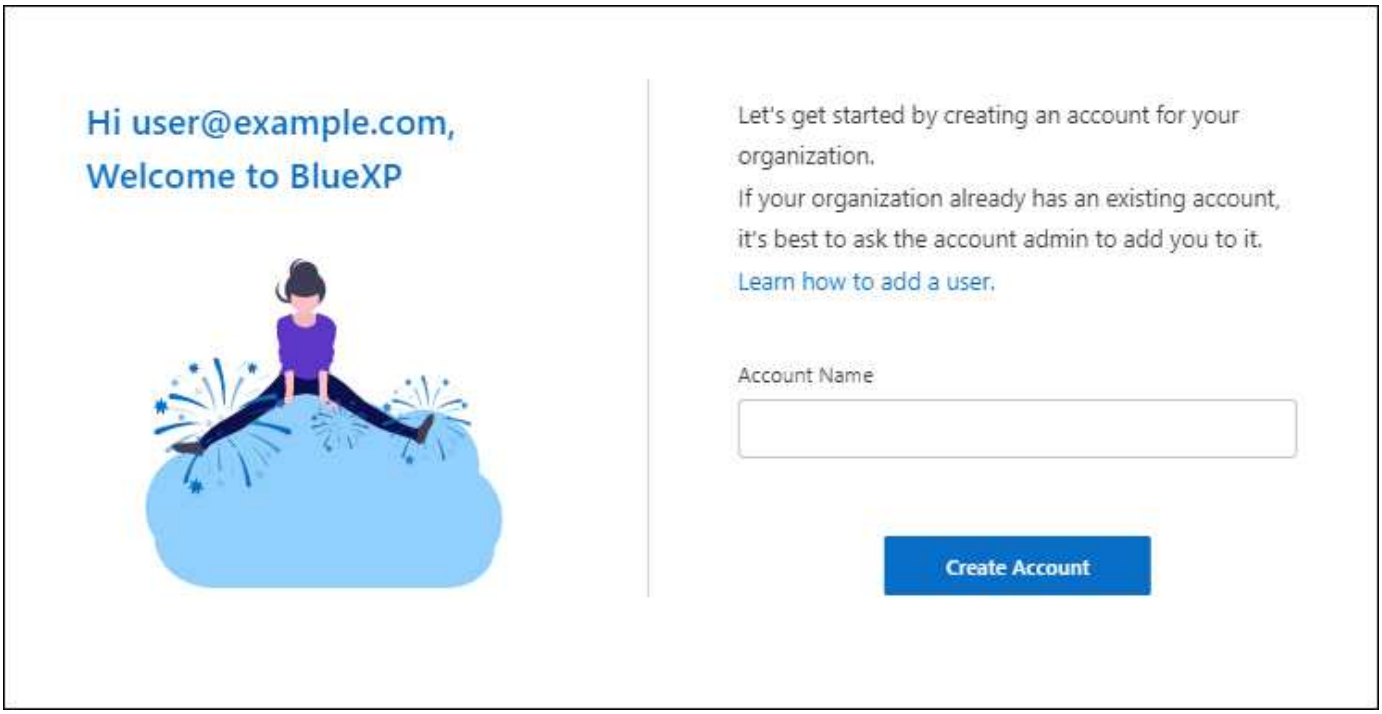
Una firma de contabilidad pública independiente certificada y un auditor de servicios examinó BlueXP y afirmó que logró los informes SOC 2 de tipo 2 basados en los criterios aplicables de los servicios de confianza.

"Consulte los informes de SOC 2 de NetApp"

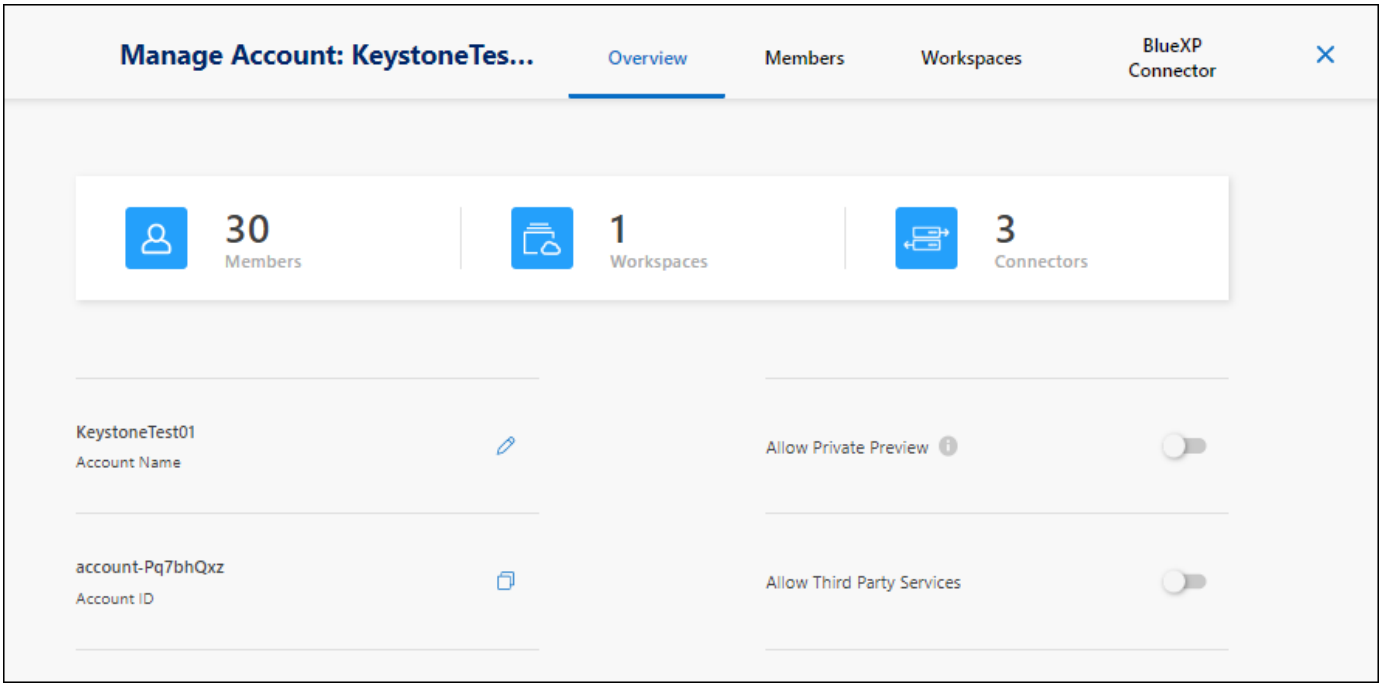
Obtenga más información sobre las cuentas de BlueXP

Una cuenta de *BlueXP* ofrece multi-tenancy a tu organización, lo que te permite organizar usuarios y recursos en *workspaces* aislados. Por ejemplo, un grupo de usuarios puede desplegar y gestionar entornos de trabajo de Cloud Volumes ONTAP en un espacio de trabajo que no es visible para los usuarios que gestionan entornos de trabajo en un espacio de trabajo diferente.

Cuando acceda por primera vez a BlueXP, se le pedirá que seleccione o cree una cuenta. Por ejemplo, verá la siguiente pantalla si aún no tiene una cuenta:



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



"Aprenda a administrar su cuenta de BlueXP".

Modos de implementación

BlueXP ofrece los siguientes modos de despliegue para su cuenta: Modo estándar, modo restringido y modo privado. Estos modos son compatibles con entornos que tienen diversos niveles de restricciones de seguridad y conectividad.

"Obtenga más información sobre los modos de implementación de BlueXP".

Miembros

Los miembros son usuarios de BlueXP que usted asocia con su cuenta de BlueXP. 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*: Solo puede ver la información de cumplimiento para la clasificación de BlueXP y generar informes para espacios de trabajo a los que tengan permiso para acceder.

"Obtenga más información sobre estos roles".

Espacios de trabajo

En BlueXP, un área de trabajo aísla cualquier número de *entornos de trabajo* de otros usuarios de la cuenta. 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

Un conector ejecuta las acciones que BlueXP necesita realizar para gestionar su infraestructura de datos. 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 haya configurado.

Puede utilizar un conector con más de un servicio BlueXP. Por ejemplo, si estás usando un conector para gestionar Cloud Volumes ONTAP, puedes utilizar ese mismo conector con otro servicio como la organización en niveles de BlueXP.

"Más información sobre conectores".

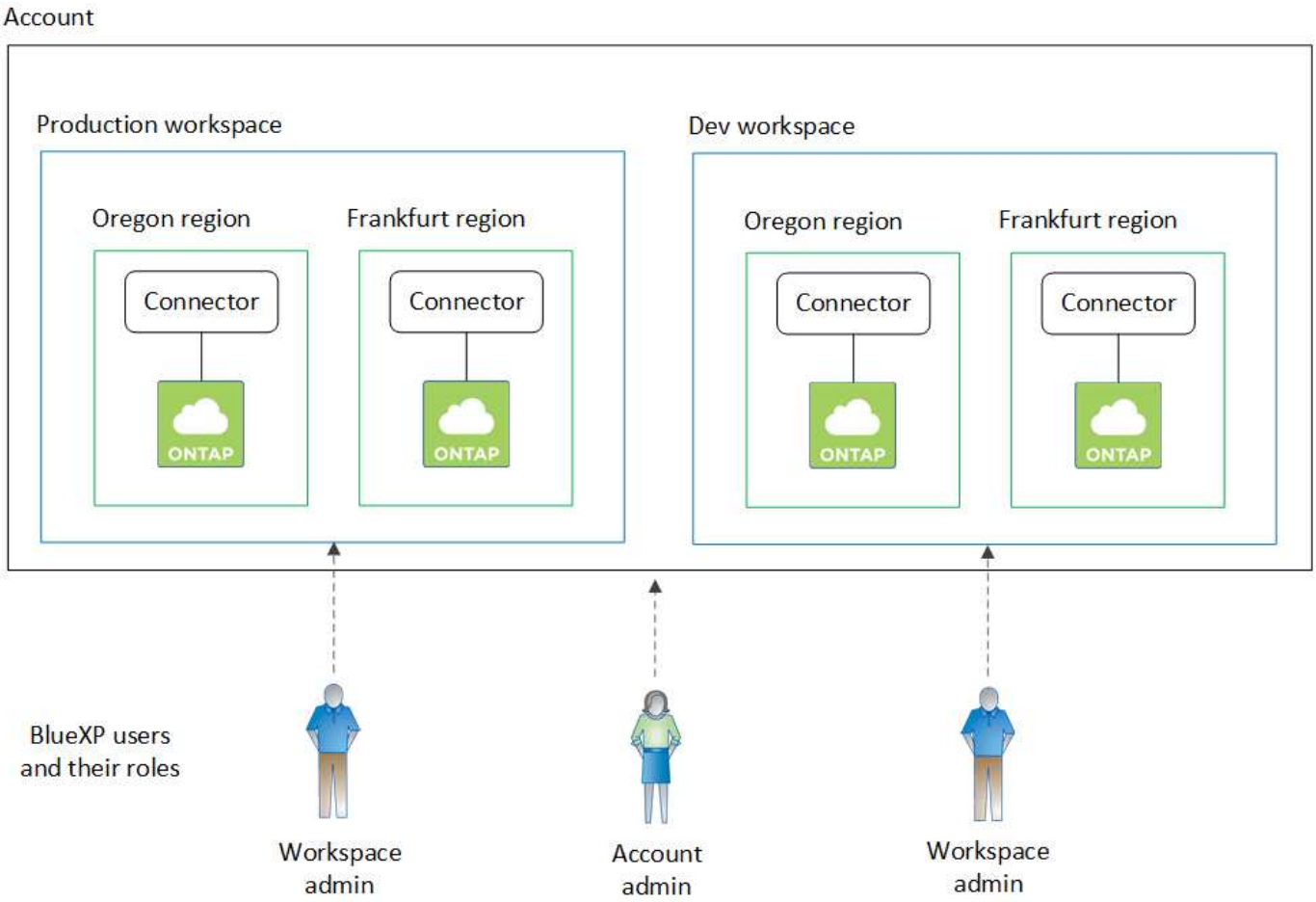
Ejemplos

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 BlueXP: Se ejecutan en un proveedor de la nube. Ésta es una representación conceptual de la relación entre cada componente.

Múltiples espacios de trabajo

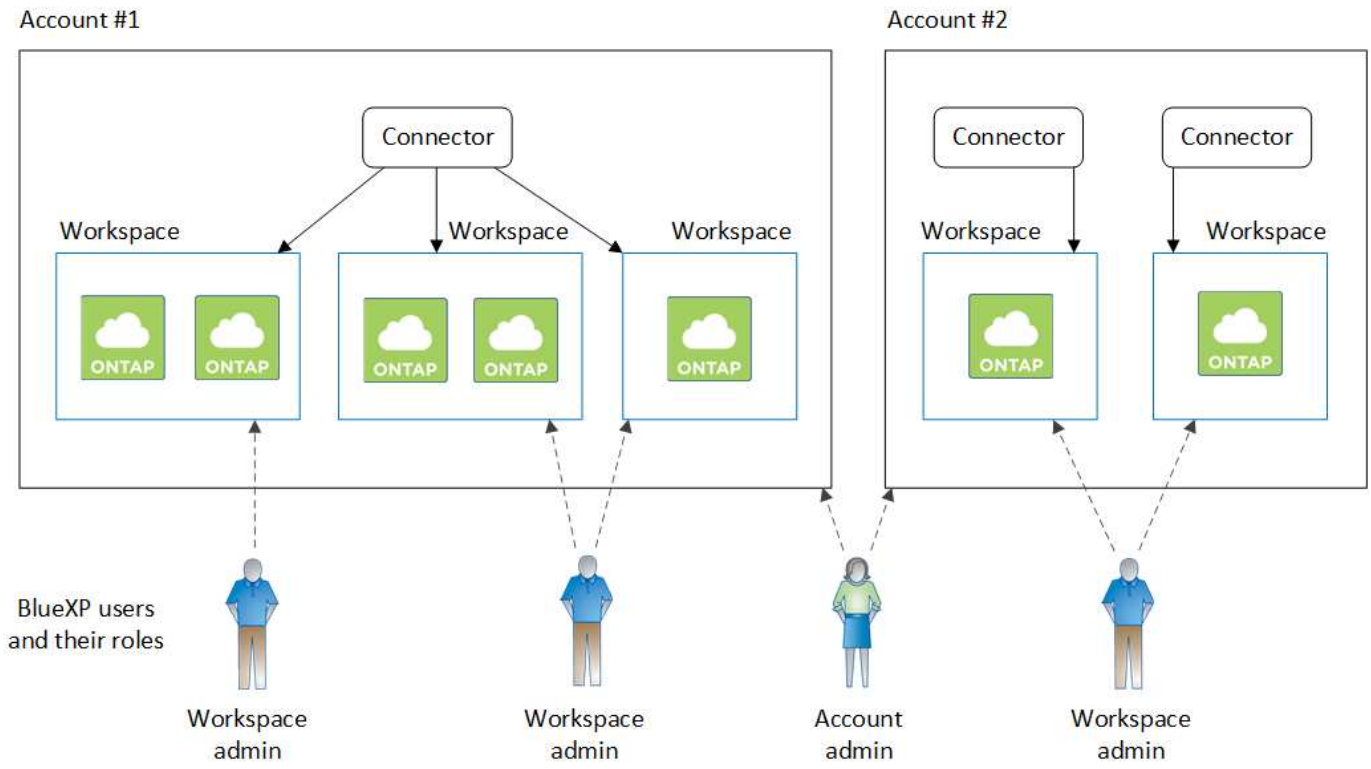
En el ejemplo siguiente se muestra una cuenta que utiliza dos espacios de trabajo para crear entornos aislados. El primer espacio de trabajo es para un entorno de producción y el segundo para un entorno de desarrollo.



Múltiples cuentas

A continuación, se muestra otro ejemplo que demuestra el nivel más alto de multi-tenancy utilizando dos cuentas separadas de BlueXP. 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.



Más información sobre conectores

Un *Connector* es el software de NetApp que se ejecuta en la red del cloud o en las instalaciones. Ejecuta las acciones que BlueXP necesita realizar para gestionar su infraestructura de datos. El conector sondea constantemente la capa SaaS BlueXP para cualquier acción que necesite tomar. No necesitas un conector para empezar con BlueXP, pero tendrás que crear un conector para desbloquear todas las funciones y servicios de BlueXP.

Lo que puede hacer sin un conector

No es necesario un conector para comenzar con BlueXP. Puede utilizar varias características y servicios dentro de BlueXP sin crear nunca un conector.

Puede utilizar las siguientes funciones y servicios de BlueXP sin un conector:

- Creación del entorno de trabajo de Amazon FSX para ONTAP de NetApp

  Aunque no es necesario que un conector cree un entorno de trabajo, es necesario crear y gestionar volúmenes, replicar datos e integrar FSx para ONTAP con servicios como la clasificación de BlueXP y la copia y sincronización de BlueXP.

- Catálogo de automatización
- Azure NetApp Files

  Aunque no es necesario un conector para configurar y gestionar Azure NetApp Files, se necesita un conector para usar la clasificación de BlueXP para analizar datos de Azure NetApp Files.

- Cloud Volumes Service para Google Cloud

- Copiar y sincronizar
- Asesor digital
- Cartera digital

  En casi todos los casos, puede agregar una licencia a la cartera digital sin un conector.

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

- 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"

- Sostenibilidad

Cuando se necesita un conector

Al utilizar BlueXP en modo estándar, se necesita un conector para las siguientes funciones y servicios de BlueXP:

- Funciones de gestión de Amazon FSX para ONTAP
- Almacenamiento Amazon S3
- Almacenamiento de Azure Blob
- Backup y recuperación
- Clasificación
- Cloud Volumes ONTAP
- Recuperación tras siniestros
- Sistemas E-Series
- Eficiencia económica [1]
- Almacenamiento en caché en el edge
- Buckets de Google Cloud Storage
- Clústeres de Kubernetes
- Informes de migración
- Integración de clústeres de ONTAP en las instalaciones con servicios de datos de BlueXP
- Resistencia operativa [1]
- Protección contra ransomware
- Sistemas StorageGRID
- Organización en niveles
- Almacenamiento en caché de volúmenes

[1] Mientras puede acceder a estos servicios sin un conector, se requiere un conector para iniciar acciones

desde los servicios.

Se necesita un conector para utilizar BlueXP en modo restringido o en modo privado.

Los conectores deben estar operativos en todo momento

Los conectores son una parte fundamental de la arquitectura de servicios de BlueXP. Es su responsabilidad asegurarse de que los conectores relevantes estén activos, operativos y accesibles en todo momento. Mientras que el servicio está diseñado para superar breves interrupciones de la disponibilidad del conector, debe tomar medidas inmediatas cuando sea necesario para solucionar fallos en la infraestructura.

Esta documentación se rige por el EULA. Si el producto no se utiliza de acuerdo con la documentación, la funcionalidad y el funcionamiento del producto, así como los derechos del usuario final, pueden verse afectados negativamente.

Impacto sobre Cloud Volumes ONTAP

Un conector es un componente clave en el estado y funcionamiento 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.

Ubicaciones admitidas

Se admite un conector en las siguientes ubicaciones:

- Amazon Web Services
- Microsoft Azure

  Un conector en Azure debe ponerse en marcha en la misma región de Azure que los sistemas de 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"

- Google Cloud

  Si desea utilizar los servicios de BlueXP con Google Cloud, debe utilizar un conector que se ejecute en Google Cloud.

- En sus instalaciones

Modo restringido y modo privado

Para utilizar BlueXP en modo restringido o privado, se inicia con BlueXP instalando el conector y, a continuación, accediendo a la interfaz de usuario que se ejecuta localmente en el conector.

"Obtenga más información sobre los modos de implementación de BlueXP".

Cómo crear un conector

Un administrador de cuentas de BlueXP puede crear un conector directamente desde BlueXP, desde el mercado de su proveedor de la nube, o instalando manualmente el software en su propio host Linux. La forma de comenzar depende de si está utilizando BlueXP en modo estándar, modo restringido o modo privado.

- "Obtenga más información sobre los modos de implementación de BlueXP"
- "Empieza a usar BlueXP en el modo estándar"
- "Empieza a usar BlueXP en modo restringido"
- "Empieza a usar BlueXP en modo privado"

Permisos

Se necesitan permisos específicos para crear el conector directamente desde BlueXP y se necesita otro conjunto de permisos para la propia instancia del conector. Si crea el conector en AWS o Azure directamente desde BlueXP, BlueXP crea el conector con los permisos que necesita.

Cuando se utiliza BlueXP en el modo estándar, la forma de proporcionar permisos depende de cómo tengas previsto crear el Connector.

Para obtener más información sobre cómo configurar permisos, consulte lo siguiente:

- Modo estándar
  - "Opciones de instalación de conectores en AWS"
  - "Opciones de instalación del conector en Azure"
  - "Opciones de instalación del conector en Google Cloud"
  - "Configure permisos en el cloud para puestas en marcha en las instalaciones"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

Para ver los permisos exactos que el conector necesita para las operaciones diarias, consulte las siguientes páginas:

- "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.

Cuando usas BlueXP en modo estándar o en modo restringido, Connector actualiza automáticamente su software a la última versión, siempre y cuando tenga acceso a Internet saliente para obtener la actualización del software. Si utiliza BlueXP en modo privado, deberá actualizar manualmente el conector.

"Aprenda a actualizar manualmente el software del conector".

Mantenimiento del sistema operativo y los equipos virtuales

El mantenimiento del sistema operativo en el host del conector es responsabilidad suya. Por ejemplo, debe aplicar actualizaciones de seguridad al sistema operativo en el host del conector siguiendo los procedimientos estándar de su empresa para la distribución del sistema operativo.

Tenga en cuenta que no es necesario detener ningún servicio en el host del conector cuando se ejecuta una actualización del SO.

Si necesita parar e iniciar el conector VM, debe hacerlo desde la consola de su proveedor de cloud o mediante los procedimientos estándar para la gestión en las instalaciones.

Tenga en cuenta que el conector debe estar operativo en todo momento.

Múltiples entornos de trabajo

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.

Múltiples 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:

- Tiene un entorno multicloud (por ejemplo, AWS y Azure) y prefiere tener 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 BlueXP para proporcionar servicios a sus clientes, mientras que usa otra cuenta para proporcionar recuperación ante desastres para una de sus unidades de negocio. Cada cuenta tendría conectores independientes.

Cuándo cambiar

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".

Recuperación tras siniestros

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.

Obtenga más información sobre los modos de implementación de BlueXP

BlueXP ofrece varios *modos de implementación* que le permiten utilizar BlueXP de forma que se adapte a sus necesidades empresariales y de seguridad. *Standard Mode* aprovecha la capa SaaS de BlueXP para proporcionar todas las funciones, mientras que *restricted mode* y *private mode* están disponibles para organizaciones que tienen restricciones de conectividad.

Mientras BlueXP inhibe el flujo del tráfico, la comunicación y los datos cuando usa modo restringido o modo privado, es responsabilidad suya asegurarse de que su entorno (en las instalaciones y en el cloud) cumpla con las normativas requeridas.

Descripción general

BlueXP ofrece los siguientes modos de implementación para su cuenta. Cada modo difiere en términos de requisitos de conectividad saliente, ubicación de implementación, proceso de instalación, método de autenticación, servicios de datos y almacenamiento disponibles y métodos de carga.

Modo estándar

BlueXP es accesible a los usuarios como servicio en nube desde la consola basada en Web. Dependiendo de los servicios de BlueXP que tenga previsto utilizar, un administrador de BlueXP crea uno o más conectores para gestionar los datos dentro de su entorno de cloud híbrido.

Este modo utiliza la transmisión de datos cifrados a través de Internet pública.

Modo restringido

Un conector BlueXP se instala en la nube (en una región gubernamental, una región soberana en nube o una región comercial) y tiene conectividad externa limitada a la capa SaaS BlueXP. Los usuarios acceden a BlueXP localmente desde la consola basada en Web que está disponible desde el conector, no desde la capa SaaS.

Este modo suele ser utilizado por los gobiernos estatales y locales y las empresas reguladas.

Obtenga más información acerca de la conectividad saliente a la capa SaaS.

Modo privado

Un conector BlueXP se instala en las instalaciones o en la nube (en una región segura, una región de nube soberana o una región comercial) y tiene conectividad *no* con la capa SaaS BlueXP. Los usuarios acceden a BlueXP localmente desde la consola basada en Web que está disponible desde el conector, no desde la capa SaaS.

Una región segura incluye "Cloud secreto de AWS", "Cloud secreto principal de AWS", y. "Azure IL6"

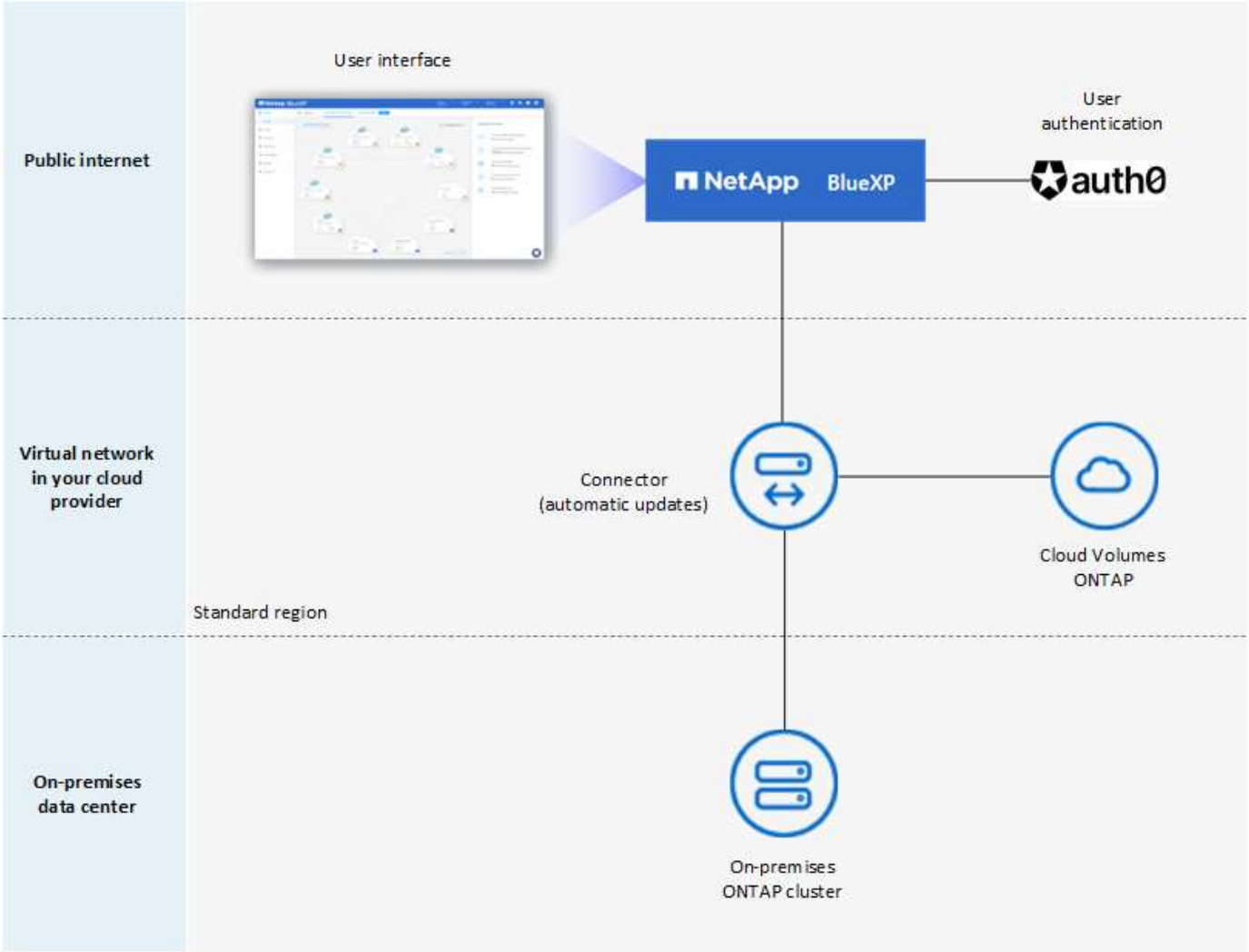
La tabla siguiente ofrece una comparación de estos modos.

	Modo estándar	Modo restringido	Modo privado
¿Es necesaria una conexión a la capa SaaS de BlueXP?	Sí	Sólo saliente	No
¿Es necesaria una conexión con su proveedor de cloud?	Sí	Sí, dentro de la región	Sí, dentro de la región (si se utiliza Cloud Volumes ONTAP)
Instalación del conector	Desde BlueXP, Cloud Marketplace o instalación manual	Cloud Marketplace o instalación manual	Instalación manual
Actualizaciones de conectores	Actualizaciones automáticas del software NetApp Connector	Actualizaciones automáticas del software NetApp Connector	Se requiere actualización manual
Acceso de interfaz de usuario	De la capa SaaS BlueXP	Localmente desde el conector VM	Localmente desde el conector VM
Extremo de API	La capa SaaS BlueXP	El conector	El conector
Autenticación	A través de SaaS mediante auth0, inicio de sesión de NSS o federación de identidades	A través de SaaS mediante auth0 o federación de identidades	Autenticación de usuario local
Almacenamiento y servicios de datos	Todos son compatibles	Muchos son compatibles	Se admiten varios
Opciones de licencia	Suscripciones de mercado y BYOL	Suscripciones de mercado y BYOL	BYOL

Lea las siguientes secciones para obtener más información sobre estos modos, como qué funciones y servicios de BlueXP son compatibles.

Modo estándar

La siguiente imagen es un ejemplo de una implementación de modo estándar.



BlueXP funciona de la siguiente manera en modo estándar:

Comunicación saliente

Se requiere conectividad desde la capa SaaS conector a BlueXP, a los recursos disponibles públicamente de su proveedor de cloud y a otros componentes esenciales para las operaciones diarias.

- "Puntos finales con los que el conector se pone en contacto en AWS"
- "Puntos finales con los que el conector se contacta en Azure"
- "Puntos finales con los que se contacta el conector en Google Cloud"

Ubicación compatible para el conector

En el modo estándar, el conector es compatible con el cloud o con las instalaciones.

Instalación del conector

Es posible instalar el conector en un asistente de configuración de BlueXP, desde AWS o Azure Marketplace, o mediante un instalador para instalar manualmente el conector en su propio host Linux en su centro de datos o en la nube.

Actualizaciones de conectores

Las actualizaciones automatizadas del software Connector están disponibles en BlueXP con actualizaciones mensuales.

Acceso a la interfaz de usuario

Puede accederse a la interfaz de usuario desde la consola basada en web que se proporciona mediante la capa SaaS.

Extremo de API

Las llamadas API se realizan en el siguiente punto final:
https://cloudmanager.cloud.netapp.com

Autenticación

La autenticación se proporciona a través del servicio cloud de BlueXP mediante auth0 o a través de inicios de sesión del sitio de soporte de NetApp (NSS). la federación de identidades está disponible.

Servicios compatibles con BlueXP

Todos los servicios de BlueXP están disponibles para los usuarios.

Opciones de licencias compatibles

Las suscripciones a Marketplace y BYOL son compatibles con el modo estándar; sin embargo, las opciones de licencia admitidas dependen del servicio BlueXP que esté utilizando. Consulte la documentación de cada servicio para obtener más información sobre las opciones de licencia disponibles.

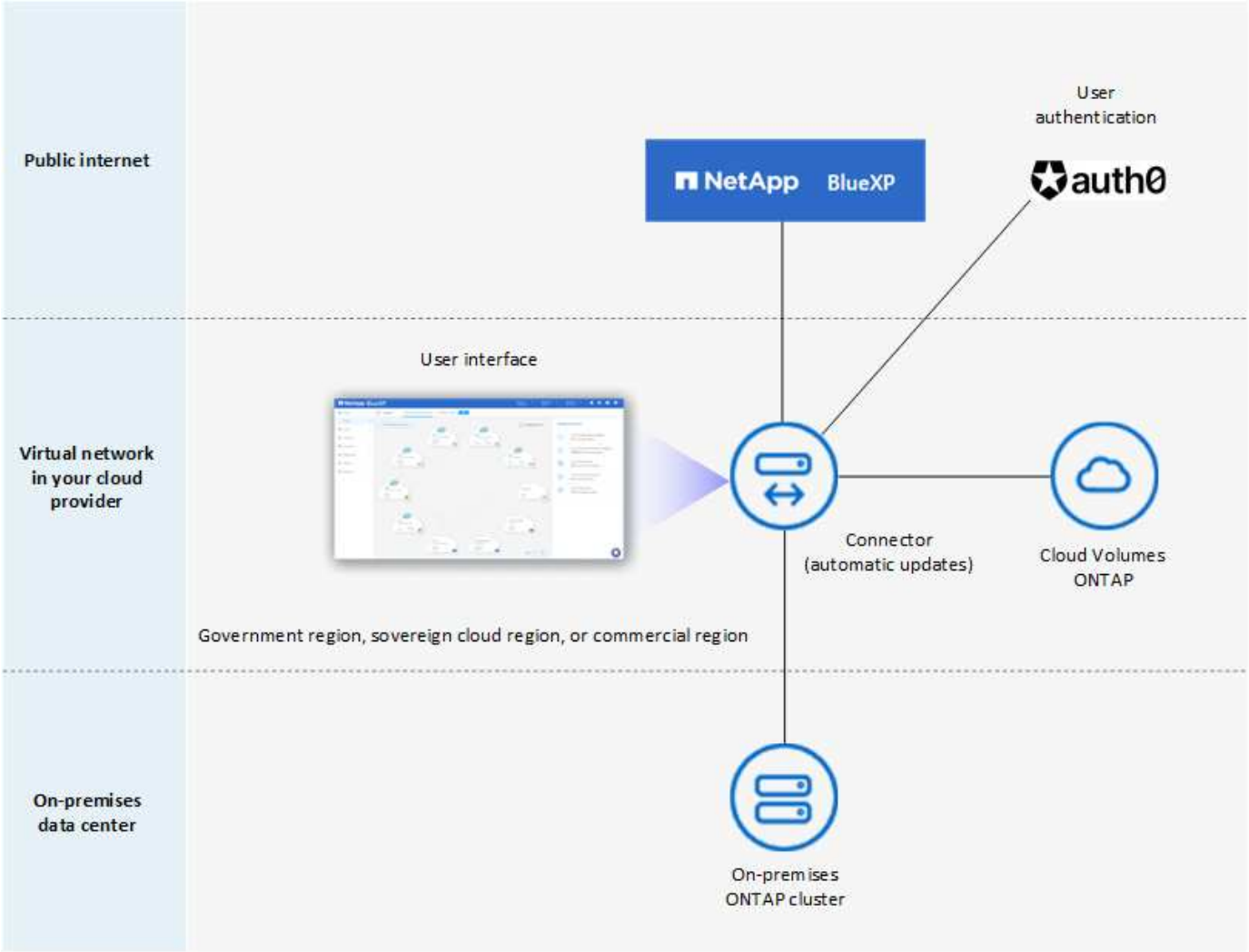
Cómo comenzar con el modo estándar

Vaya a la "Consola BlueXP basada en Web" y regístrese.

"Aprenda cómo empezar a utilizar el modo estándar".

Modo restringido

La siguiente imagen es un ejemplo de implementación de modo restringido.



BlueXP funciona de la siguiente manera en modo restringido:

Comunicación saliente

Se requiere conectividad saliente desde el conector hasta la capa SaaS BlueXP para utilizar servicios de datos BlueXP, para habilitar actualizaciones de software automáticas del conector, para utilizar autenticación basada en auth0 y para enviar metadatos con fines de carga (nombre de VM de almacenamiento, capacidad asignada y UUID de volumen, tipo e IOPS).

La capa SaaS BlueXP no inicia la comunicación al conector. Toda la comunicación la inicia el conector, que puede extraer o insertar datos de o a la capa SaaS según sea necesario.

También es necesario establecer una conexión con recursos de proveedor de cloud desde la región.

Ubicación compatible para el conector

En el modo restringido, el conector es compatible con la nube: En una región gubernamental, soberana o comercial.

Instalación del conector

Es posible instalar el conector en AWS o Azure Marketplace o una instalación manual en su propio host Linux.

Actualizaciones de conectores

Las actualizaciones automatizadas del software Connector están disponibles en BlueXP con actualizaciones mensuales.

Acceso a la interfaz de usuario

Se puede acceder a la interfaz de usuario desde la máquina virtual de Connector que se implementa en la región de la nube.

Extremo de API

Se realizan llamadas API a la máquina virtual Connector.

Autenticación

La autenticación se proporciona a través del servicio en la nube de BlueXP con auth0. la federación de identidades también está disponible.

Servicios compatibles con BlueXP

BlueXP admite los siguientes servicios de almacenamiento y datos con modo restringido:

Servicios compatibles	Notas
Amazon FSX para ONTAP	Soporte completo
Azure NetApp Files	Soporte completo
Backup y recuperación	Se admite en regiones gubernamentales y regiones comerciales con modo restringido. No se admite en regiones soberanas con modo restringido. En el modo restringido, el backup y la recuperación de BlueXP solo admiten backup y restauración de datos de volúmenes de ONTAP. "Consulte la lista de destinos de backup admitidos para los datos de ONTAP" No se admiten los backups y la restauración de datos de aplicaciones, datos de máquinas virtuales y datos de Kubernetes.
Clasificación	Compatible en regiones gubernamentales con modo restringido. No se admite en regiones comerciales o en regiones soberanas con modo restringido. Se aplican las siguientes limitaciones: • Las cuentas de OneDrive, cuentas de SharePoint y cuentas de Google Drive no se pueden analizar. • La funcionalidad de etiqueta de Microsoft Azure Information Protection (AIP) no se puede integrar.
Cloud Volumes ONTAP	Soporte completo

Servicios compatibles	Notas
Cartera digital	Puede utilizar la cartera digital con las opciones de licencia admitidas que se indican a continuación para el modo restringido.
Clústeres de ONTAP en las instalaciones	Se admiten tanto la detección con un conector como la detección sin un conector (detección directa). Cuando detecta un clúster en las instalaciones con un conector, la vista avanzada (System Manager) no es compatible.
Replicación	Compatible en regiones gubernamentales con modo restringido. No se admite en regiones comerciales o en regiones soberanas con modo restringido.

Opciones de licencias compatibles

Las siguientes opciones de licencia son compatibles con el modo restringido:

- Suscripciones al mercado (contratos por horas y anuales)

  Tenga en cuenta lo siguiente:

  - Para Cloud Volumes ONTAP, solo es compatible con las licencias basadas en capacidad.
  - En Azure, los contratos anuales no son compatibles con las regiones gubernamentales.
- BYOL

  Para Cloud Volumes ONTAP, tanto las licencias basadas en capacidad como las basadas en nodos son compatibles con BYOL.

Cómo comenzar con el modo restringido

Debe habilitar el modo restringido al crear su cuenta de BlueXP.

Si aún no tiene una cuenta, se le pedirá que cree su cuenta y habilite el modo restringido cuando inicie sesión en BlueXP por primera vez desde un conector que instaló manualmente o que creó desde el mercado de su proveedor de la nube.

Si ya tiene una cuenta y desea crear otra, debe utilizar la API de soporte.

Tenga en cuenta que no puede cambiar la configuración de modo restringido después de que BlueXP cree la cuenta. No se puede activar el modo restringido más adelante y no se puede desactivar más adelante. Se debe establecer en el momento de crear la cuenta.

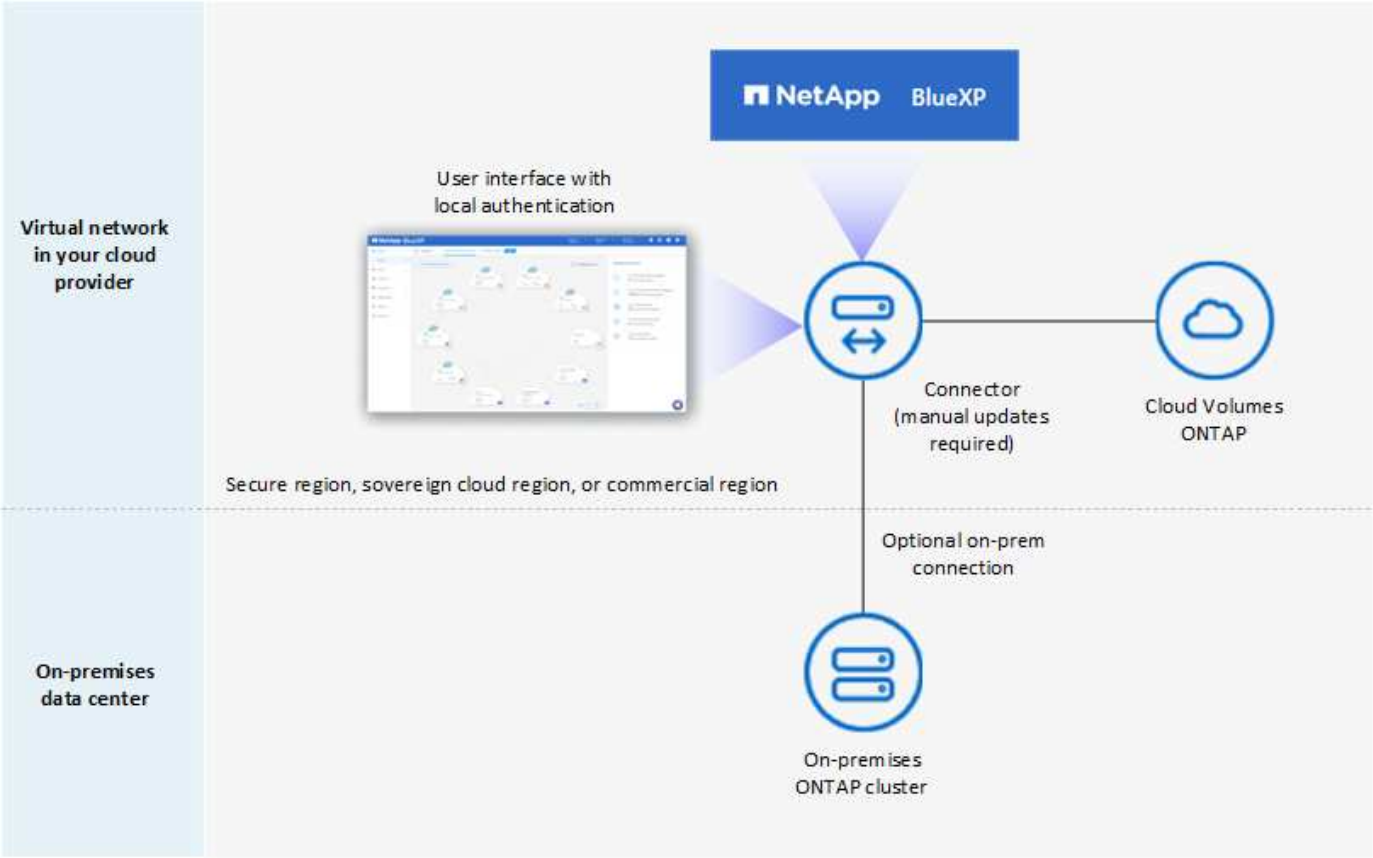
- "Aprenda a empezar a utilizar el modo restringido".
- "Aprenda a crear una cuenta de BlueXP adicional".

Modo privado

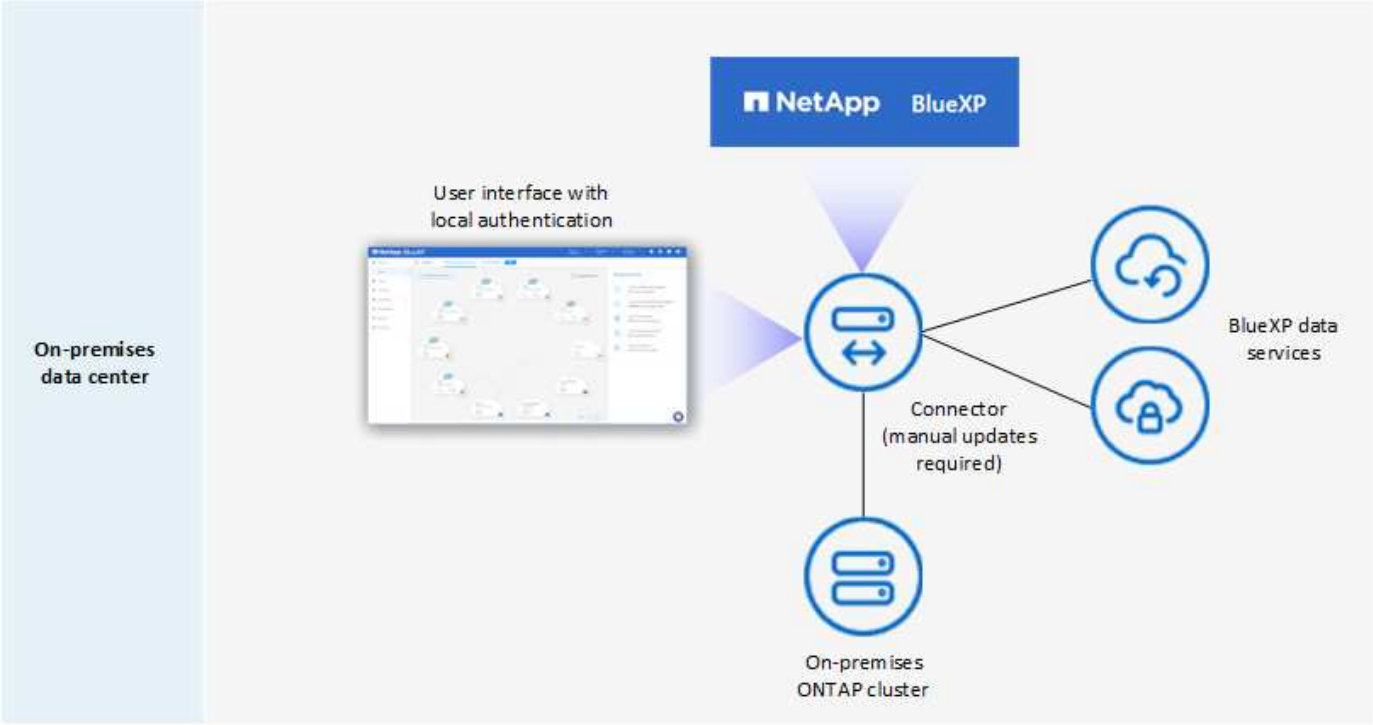
En modo privado, puede instalar un conector en las instalaciones o en el cloud y, a continuación, utilizar BlueXP para gestionar los datos en su cloud híbrido. No hay conectividad con la capa SaaS BlueXP.

En la siguiente imagen, se muestra un ejemplo de puesta en marcha en modo privado en la que se instala el

conector en el cloud y se gestiona tanto Cloud Volumes ONTAP como un clúster ONTAP en las instalaciones.



Mientras tanto, la segunda imagen muestra un ejemplo de implementación de modo privado en la que el conector está instalado en las instalaciones, administra un clúster ONTAP en las instalaciones y proporciona acceso a servicios de datos BlueXP compatibles.



BlueXP funciona de la siguiente manera en modo privado:

Comunicación saliente

No se requiere conectividad saliente en la capa de BlueXP SaaS. Todos los paquetes, dependencias y componentes esenciales se empaquetan con el conector y se sirven desde la máquina local. La conectividad con los recursos disponibles públicamente de su proveedor de cloud es obligatoria únicamente si se pone en marcha Cloud Volumes ONTAP.

Ubicación compatible para el conector

En modo privado, el conector es compatible con el cloud o el entorno local.

Instalación del conector

Las instalaciones manuales del conector son compatibles con su propio host Linux, tanto en el cloud como en las instalaciones.

Actualizaciones de conectores

Debe actualizar el software del conector manualmente. El software del conector se publica en el sitio de soporte de NetApp a intervalos no definidos.

Acceso a la interfaz de usuario

Puede accederse a la interfaz de usuario desde el conector que ha implementado en su región de cloud o en sus instalaciones.

Extremo de API

Se realizan llamadas API a la máquina virtual Connector.

Autenticación

La autenticación se proporciona mediante la gestión y el acceso de usuarios locales. La autenticación no se proporciona a través del servicio en la nube de BlueXP.

Servicios de BlueXP compatibles en las implementaciones de cloud

BlueXP admite los siguientes servicios de almacenamiento y datos con modo privado cuando el conector está instalado en la nube:

Servicios compatibles	Notas
Backup y recuperación	Compatible con regiones comerciales de AWS y Azure. No es compatible con Google Cloud ni en "Cloud secreto de AWS", "Cloud secreto principal de AWS", o. "Azure IL6" En el modo privado, el backup y la recuperación de BlueXP admite solo backup y restauración de datos de volúmenes de ONTAP. "Consulte la lista de destinos de backup admitidos para los datos de ONTAP" No se admiten los backups y la restauración de datos de aplicaciones, datos de máquinas virtuales y datos de Kubernetes.

Servicios compatibles	Notas
Cloud Volumes ONTAP	Como no hay acceso a Internet, las siguientes funciones no están disponibles: Actualizaciones de software automatizadas y AutoSupport.
Cartera digital	Puede utilizar la cartera digital con las opciones de licencia admitidas que se indican a continuación para el modo privado.
Clústeres de ONTAP en las instalaciones	Requiere conectividad desde el cloud (donde está instalado el conector) al entorno local. No se admite la detección sin conector (detección directa).

Servicios de BlueXP compatibles en implementaciones locales

BlueXP admite los siguientes servicios de almacenamiento y datos con modo privado cuando el conector está instalado en sus instalaciones:

Servicios compatibles	Notas
Backup y recuperación	En el modo privado, el backup y la recuperación de BlueXP admite solo backup y restauración de datos de volúmenes de ONTAP. "Consulte la lista de destinos de backup admitidos para los datos de volúmenes ONTAP" No se admiten los backups y la restauración de datos de aplicaciones, datos de máquinas virtuales y datos de Kubernetes.
Clasificación	• Las únicas fuentes de datos admitidas son las que se pueden detectar localmente. "Ver las fuentes que puede descubrir localmente" • Las funciones que requieren acceso saliente a Internet no son compatibles. "Vea las limitaciones de la función"
Cartera digital	Puede utilizar la cartera digital con las opciones de licencia admitidas que se indican a continuación para el modo privado.
Clústeres de ONTAP en las instalaciones	No se admite la detección sin conector (detección directa).
Replicación	Soporte completo

Opciones de licencias compatibles

Solo BYOL es compatible con el modo privado.

Para BYOL de Cloud Volumes ONTAP, solo las licencias basadas en nodos son compatibles. No se admite la gestión de licencias basadas en capacidad. Como no hay disponible una conexión a Internet de salida, deberá cargar manualmente el archivo de licencia de Cloud Volumes ONTAP en la cartera digital de BlueXP.

"Descubre cómo añadir licencias a la cartera digital de BlueXP"

Cómo comenzar con el modo privado

Para acceder al modo privado, descargue el instalador "sin conexión" del sitio de soporte de NetApp.

"Aprenda cómo empezar a utilizar el modo privado".

> Si desea utilizar BlueXP en "Cloud secreto de AWS" o la "Cloud secreto principal de AWS", entonces debe seguir instrucciones separadas para comenzar en esos entornos. "Descubra cómo empezar a utilizar Cloud Volumes ONTAP en el cloud secreto de AWS o en el cloud secreto superior"

Comparación de servicios y características

La tabla siguiente puede ayudarle a identificar rápidamente qué servicios y funciones de BlueXP son compatibles con el modo restringido y el modo privado.

Tenga en cuenta que algunos servicios pueden ser compatibles con limitaciones. Para obtener más información sobre cómo se admiten estos servicios con el modo restringido y el modo privado, consulte las secciones anteriores.

Área de producto	Servicio o característica BlueXP	Modo restringido	Modo privado
Entornos de trabajo Esta parte de la tabla enumera soporte para la gestión del entorno de trabajo desde el lienzo de BlueXP. No indica los destinos de backup admitidos para el backup y recuperación de BlueXP.	Amazon FSX para ONTAP	Sí	No
	Amazon S3	No	No
	Azure Blob	No	No
	Azure NetApp Files	Sí	No
	Cloud Volumes ONTAP	Sí	Sí
	Cloud Volumes Service para Google Cloud	No	No
	Google Cloud Storage	No	No
	Clústeres de Kubernetes	No	No
	Clústeres de ONTAP en las instalaciones	Sí	Sí
	E-Series	No	No
	StorageGRID	No	No

Área de producto	Servicio o característica BlueXP	Modo restringido	Modo privado
Servicios	Backup y recuperación	Sí "Consulte la lista de destinos de backup admitidos para los datos de volúmenes ONTAP"	Sí "Consulte la lista de destinos de backup admitidos para los datos de volúmenes ONTAP"
	Clasificación	Sí	Sí
	Operaciones de cloud	No	No
	Copiar y sincronizar	No	No
	Asesor digital	No	No
	Cartera digital	Sí	Sí
	Recuperación tras siniestros	No	No
	Eficiencia económica	No	No
	Almacenamiento en caché en el edge	No	No
	Informes de migración	No	No
	Resiliencia operativa	No	No
	Protección contra ransomware	No	No
	Replicación	Sí	Sí
	Sostenibilidad	No	No
	Organización en niveles	No	No
	Almacenamiento en caché de volúmenes	No	No
* Características*	Credenciales	Sí	Sí
	Cuentas de NSS	Sí	No
	Notificaciones	Sí	No
	Búsqueda	Sí	No
	Línea de tiempo	Sí	Sí

Comience con el modo estándar

Flujo de trabajo inicial (modo estándar)

Empieza a usar BlueXP en el modo estándar preparando redes para la consola de BlueXP, registrando y creando una cuenta, opcionalmente creando un conector y suscribiéndose a BlueXP.

En el modo estándar, los usuarios pueden acceder a BlueXP como un servicio en la nube desde la consola basada en web. Antes de empezar, debería comprender "Cuentas BlueXP", "Conectores", y. "modos de despliegue".

1 **"Prepare las redes para usar la consola de BlueXP"**

Los equipos que accedan a la consola de BlueXP deberían tener conexiones a extremos específicos para completar algunas tareas administrativas. Si la red restringe el acceso saliente, debe asegurarse de que se permiten estos puntos finales.

2 **"Regístrese y cree una cuenta"**

Vaya a la "Consola BlueXP" y regístrese. Se le dará la opción de crear una cuenta, pero puede omitir ese paso si está siendo invitado a una cuenta existente.

En este momento, ha iniciado sesión y puede empezar a utilizar varios servicios de BlueXP como Digital Advisor, Amazon FSX para ONTAP, Azure NetApp Files y muchos más. "Aprenda lo que puede hacer sin un conector".

3 **Cree un conector**

No necesita un conector para comenzar con BlueXP, pero puede crear un conector para desbloquear todas las funciones y servicios de BlueXP. La conexión es el software de NetApp que permite a BlueXP gestionar recursos y procesos dentro de su entorno de cloud híbrido.

Un administrador de cuentas de BlueXP puede crear un conector en la nube o en la red local.

- "Obtenga más información sobre cuándo se necesitan los conectores y cómo trabajo"
- "Aprenda a crear un conector en AWS"
- "Aprenda a crear un conector en Azure"
- "Descubra cómo crear un conector en Google Cloud"
- "Aprenda a crear un conector en las instalaciones"

Tenga en cuenta que si desea utilizar los servicios de BlueXP para gestionar el almacenamiento y los datos en Google Cloud, el conector debe estar ejecutándose en Google Cloud.

4 **"Suscríbase a BlueXP"**

Suscríbase a BlueXP en el mercado de su proveedor de la nube para pagar los servicios de BlueXP a una tarifa por hora (PAYGO) o a través de un contrato anual.

Prepare las redes para usar la consola de BlueXP

Al usar la consola basada en web de BlueXP que se proporciona a través de la capa SaaS, se pone en contacto con varios extremos cuando completa unas pocas tareas administrativas. Los equipos que accedan a la consola de BlueXP deben tener conexiones a estos extremos.

Estos extremos se ponen en contacto desde el equipo de un usuario al completar acciones específicas desde la consola de BlueXP. También debes consultar los requisitos de red para el conector y para servicios de BlueXP específicos. Para obtener más información, consulte los enlaces relacionados al final de esta página.

Puntos finales	Específico
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	Su navegador web se pone en contacto con estas URL cuando utiliza la consola basada en web de BlueXP.
https://aiq.netapp.com	Es necesario acceder al asesor digital de BlueXP.
Servicios de AWS (amazonaws.com): • Formación CloudFormation • 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.

Más allá de estos puntos finales, también debe asegurarse de que Connector tiene acceso a Internet saliente para contactar puntos finales específicos para las operaciones diarias. Puede encontrar la lista de estos puntos finales siguiendo los enlaces de la siguiente sección.

Enlaces relacionados

- Prepare la conexión a redes para el conector

- "Configure las redes de AWS"
- "Configure las redes de Azure"
- "Configure las redes de Google Cloud"
- "Configure las redes en las instalaciones"

- Prepare las redes para los servicios de BlueXP

  Consulta la documentación para cada servicio de BlueXP.

  "Documentación de BlueXP"

Regístrese en BlueXP

BlueXP es accesible desde una consola basada en Web. Cuando comience a utilizar BlueXP, su primer paso consiste en registrarse con sus credenciales actuales del sitio de soporte de NetApp o mediante la creación de un inicio de sesión en cloud de NetApp.

Acerca de esta tarea

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). Puede configurar una conexión de federación después de registrarse. "Aprenda a usar la federación de identidades con BlueXP".

Pasos

1. Abra un explorador web y vaya al "Consola BlueXP"
2. Si tienes una cuenta del sitio de soporte de NetApp, introduce la dirección de correo electrónico asociada con tu cuenta de NSS directamente en la página **Iniciar sesión**.

   Puede omitir la página de registro si tiene una cuenta NSS. BlueXP te inscribirá como parte de este inicio de sesión inicial.

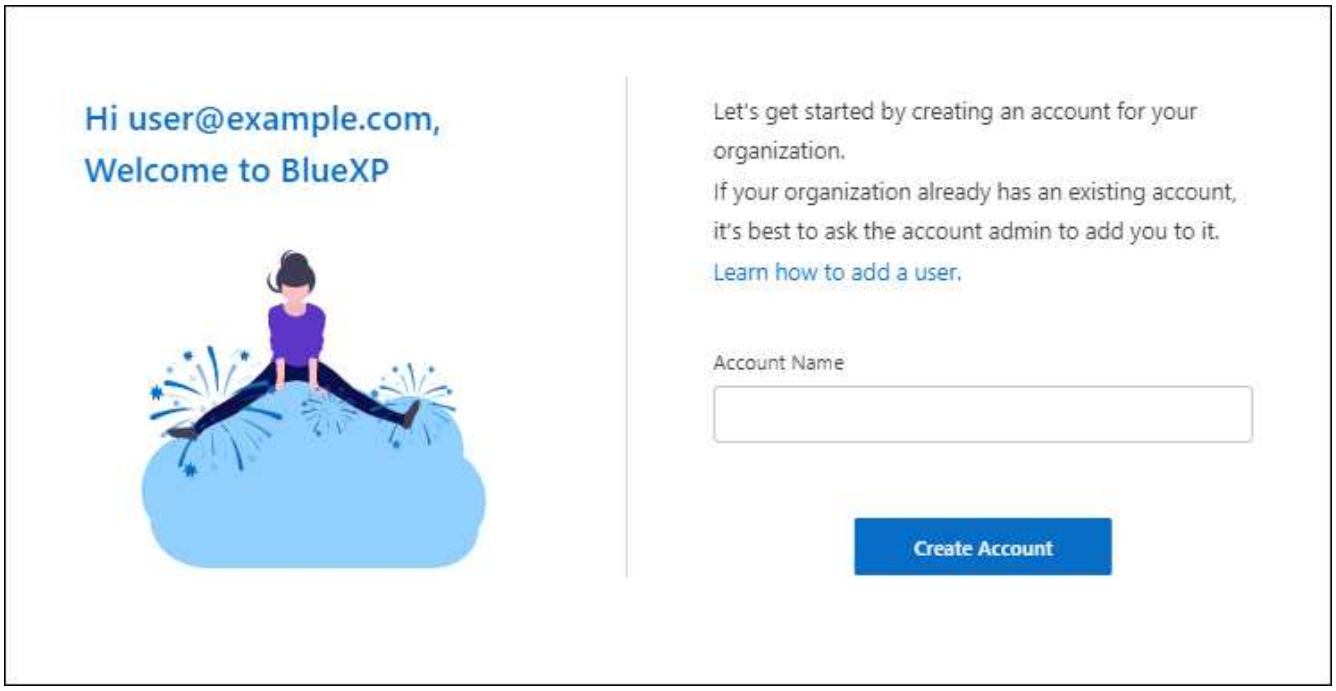
3. Si no tienes una cuenta NSS y quieres registrarte mediante la creación de un inicio de sesión en la nube de NetApp, selecciona **Regístrate**.
4. En la página **Sign up**, introduzca la información necesaria para crear un inicio de sesión en el cloud de NetApp.

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

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

   Si su negocio ya tiene una cuenta y desea unirse a ella, entonces usted debe cerrar fuera de BlueXP 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.



7. 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.

Cree un conector

AWS

Opciones de instalación de conectores en AWS

Hay varias formas diferentes de crear un conector en AWS. Directamente desde BlueXP es la forma más común.

Están disponibles las siguientes opciones de instalación:

- "Crea el conector directamente desde BlueXP" (esta es la opción estándar)

  Esta acción inicia una instancia de EC2 con Linux y el software Connector en un VPC de su elección.

- "Cree un conector desde AWS Marketplace"

  Esta acción también inicia una instancia de EC2 que ejecuta Linux y el software Connector, pero la puesta en marcha se inicia directamente desde AWS Marketplace en lugar de desde BlueXP.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará a la forma en que se prepara para la instalación. Esto incluye cómo proporciona BlueXP los permisos necesarios para autenticar y gestionar recursos en AWS.

Cree un conector en AWS desde BlueXP

Para crear un conector en AWS desde BlueXP, debe configurar la red, preparar los permisos de AWS y, a continuación, crear el conector.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

VPC y subred

Al crear el conector, es necesario especificar el VPC y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://support.netapp.com https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para actualizar el conector y sus componentes de Docker.

Extremos en los que se han contactado desde la consola de BlueXP

A medida que utiliza la consola basada en Web BlueXP que se proporciona a través de la capa SaaS, se pone en contacto con varios extremos para completar las tareas de gestión de datos. Esto incluye los extremos que se ponen en contacto para poner en marcha el conector desde la consola de BlueXP.

"Consulte la lista de extremos con los que se ha contactado desde la consola de BlueXP".

Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Configure los permisos 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, el primer paso es crear una política de IAM. Esta directiva sólo contiene los permisos necesarios para iniciar la instancia de Connector en AWS desde BlueXP.

Si es necesario, puede restringir la política de IAM mediante el IAM `Condition` elemento. "Documentación de AWS: Elemento de condición"

Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos a la instancia de Connector que permite al conector gestionar recursos de AWS.

Pasos

1. Vaya a la consola IAM de AWS.
2. Selecciona **Políticas > Crear política**.
3. Selecciona **JSON**.
4. Copie y pegue la siguiente política:

   A modo de recordatorio, esta política solo contiene los permisos necesarios para iniciar la instancia de Connector en AWS desde BlueXP. "Permite ver los permisos necesarios para la propia instancia del conector".

```
{
  "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",
        "iam:ListRoles",
        "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",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
```

```
            "ec2:TerminateInstances"
          ],
          "Condition": {
            "StringLike": {
              "ec2:ResourceTag/OCCMInstance": "*"
            }
          },
          "Resource": [
            "arn:aws:ec2:*:*:instance/*"
          ]
        }
      ]
    }
```

5. Seleccione **Siguiente** y agregue etiquetas, si es necesario.
6. Selecciona **Siguiente** e introduce un nombre y una descripción.
7. Seleccione **Crear política**.
8. Adjunte la política a una función de IAM que BlueXP puede asumir o a un usuario de IAM para que pueda proporcionar claves de acceso a BlueXP:
   - (Opción 1) Configurar una función de IAM que BlueXP puede asumir:
     i. Vaya a la consola AWS IAM de la cuenta de destino.
     ii. En Access Management, seleccione **roles > Crear función** y siga los pasos para crear la función.
     iii. En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
     iv. Seleccione **otra cuenta de AWS** e introduzca el ID de la cuenta de BlueXP SaaS: 952013314444
     v. Seleccione la directiva que ha creado en la sección anterior.
     vi. Después de crear la función, copie la función ARN para que pueda pegarla en BlueXP al crear el conector.
   - (Opción 2) Configurar permisos para un usuario de IAM para que pueda proporcionar claves de acceso a BlueXP:
     i. Desde la consola de AWS IAM, seleccione **Usuarios** y, a continuación, seleccione el nombre de usuario.
     ii. Selecciona **Añadir permisos > Adjuntar políticas existentes directamente**.
     iii. Seleccione la política que ha creado.
     iv. Seleccione **Siguiente** y luego seleccione **Agregar permisos**.
     v. Asegúrese de disponer de la clave de acceso y la clave secreta para el usuario del IAM.

Resultado

Ahora debe tener un rol de IAM que tenga los permisos necesarios o un usuario de IAM que tenga los permisos necesarios. Al crear el conector desde BlueXP, puede proporcionar información sobre la función o las claves de acceso.

Paso 3: Crear el conector

Crea el Connector directamente desde la consola basada en web de BlueXP.

Acerca de esta tarea

Al crear el conector desde BlueXP se implementa una instancia de EC2 en AWS con una configuración predeterminada. Después de crear el conector, no debe cambiar a un tipo de instancia EC2 más pequeño que tenga menos CPU o RAM. "Obtenga información sobre la configuración predeterminada para el conector".

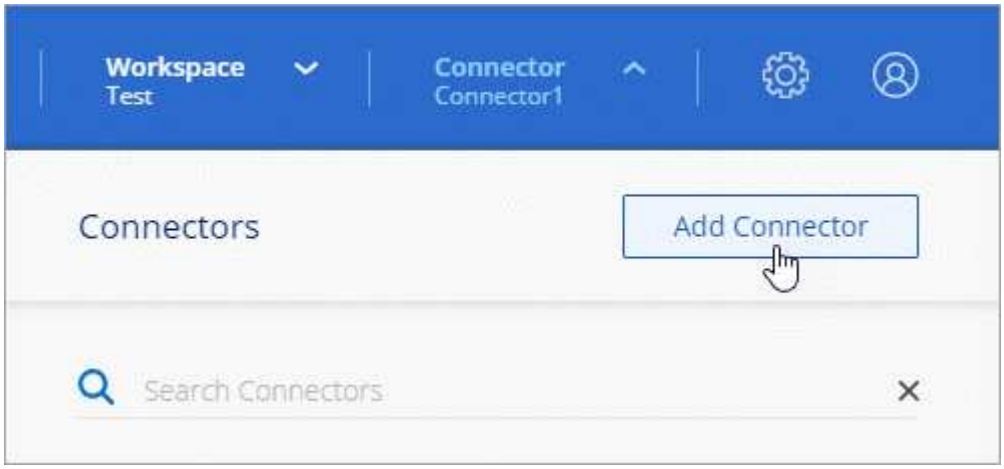
Antes de empezar

Debe tener lo siguiente:

- Un método de autenticación de AWS: Un rol de IAM o claves de acceso para un usuario IAM con los permisos necesarios.
- Un VPC y una subred que cumplan los requisitos de red.
- Una pareja de claves para la instancia de EC2.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector.

Pasos

1. Seleccione la lista desplegable **Connector** y seleccione **Add Connector**.



2. Elija **Amazon Web Services** como su proveedor de nube y seleccione **Continuar**.
3. En la página **despliegue de un conector**, revise los detalles sobre lo que necesitará. Dispone de dos opciones:
   a. Seleccione **Continuar** para prepararse para la implementación mediante la guía del producto. Cada paso de la guía del producto incluye la información que se incluye en esta página de la documentación.
   b. Selecciona **Saltar a la implementación** si ya lo preparaste 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.

  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 las reglas entrantes y salientes requeridas.

  "Ver reglas de grupos de seguridad para AWS".

- **Revisión**: Revise sus selecciones para verificar que su configuración es correcta.

5. Seleccione **Agregar**.

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

Resultado

Una vez completado el proceso, el conector está disponible para su uso en BlueXP.

Si tienes buckets de Amazon S3 en la misma cuenta de AWS en la que creaste el conector, verás que aparece automáticamente un entorno de trabajo de Amazon S3 en el lienzo de BlueXP. "Descubre cómo gestionar buckets S3 de BlueXP"

Cree un conector desde AWS Marketplace

Para crear un conector desde AWS Marketplace, debe configurar la red, preparar los permisos de AWS, revisar los requisitos de la instancia y, a continuación, crear el conector.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

VPC y subred

Al crear el conector, es necesario especificar el VPC y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://support.netapp.com https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	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 de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Configure los permisos de AWS

Para preparar una implementación de Marketplace, cree políticas de IAM en AWS y adjuntarlas a una función de IAM. Al crear el conector desde AWS Marketplace, se le pedirá que seleccione ese rol de IAM.

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:
   a. Selecciona **Políticas > Crear política**.
   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".
   c. Finalice los pasos restantes para crear la directiva.

      Dependiendo de los servicios de BlueXP que tenga previsto utilizar, puede que necesite crear una segunda política. 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. "Obtenga más información sobre las políticas de IAM para el conector".

3. Cree un rol IAM:
   a. Selecciona **Roles > Crear rol**.
   b. Seleccione **Servicio AWS > EC2**.
   c. Agregue permisos asociando la directiva que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

Resultado

Ahora tiene el rol de IAM que se puede asociar a la instancia de EC2 durante la implementación desde AWS Marketplace.

Paso 3: Revise los requisitos de la instancia

Al crear el conector, debe elegir un tipo de instancia EC2 que cumpla los siguientes requisitos.

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.

Paso 4: Crear el conector

Cree el conector directamente desde AWS Marketplace.

Acerca de esta tarea

Al crear el conector desde AWS Marketplace se implementa una instancia EC2 en AWS con una configuración predeterminada. "Obtenga información sobre la configuración predeterminada para el conector".

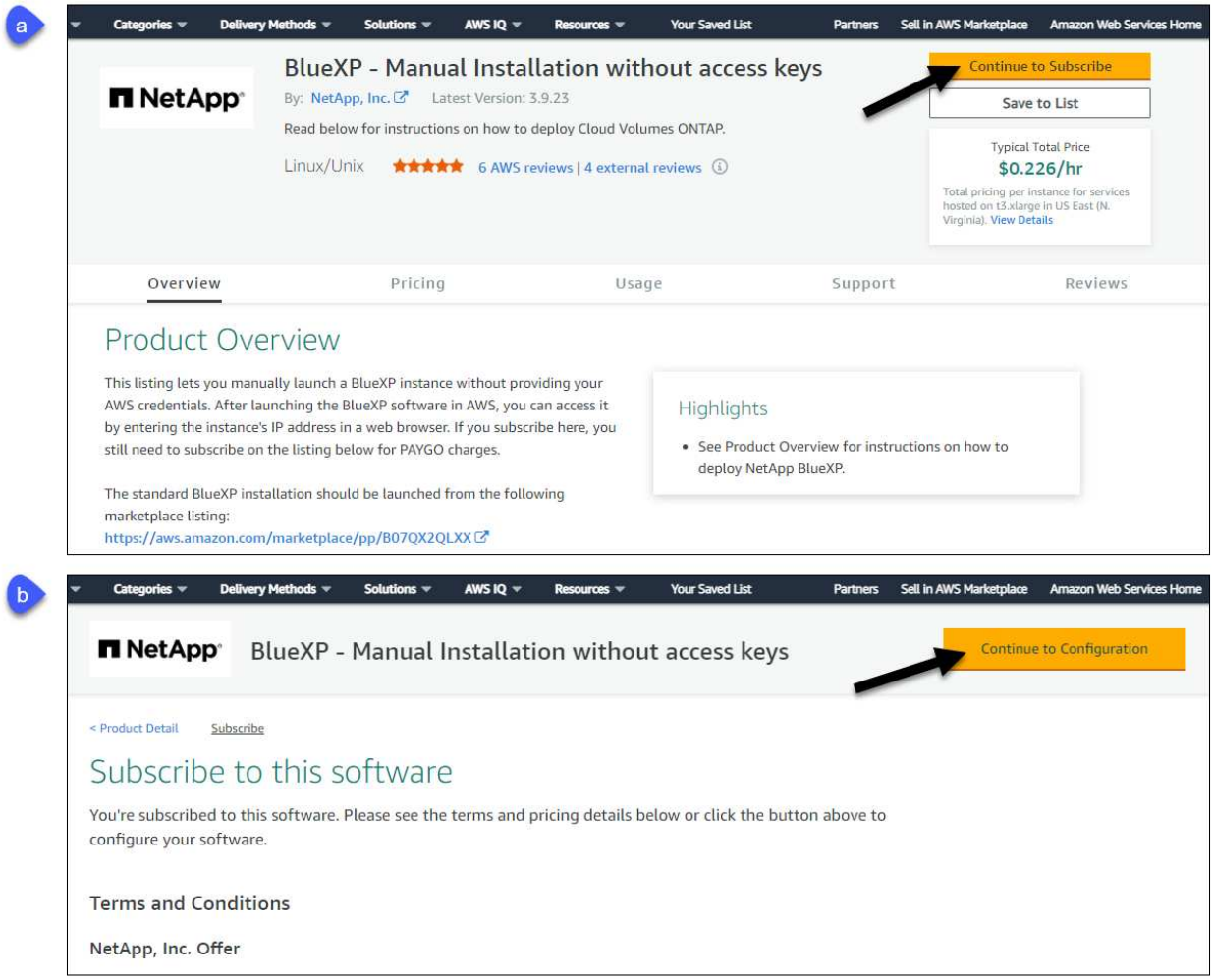
Antes de empezar

Debe tener lo siguiente:

- Un VPC y una subred que cumplan los requisitos de red.
- Función IAM con una directiva adjunta que incluye los permisos necesarios para el conector.
- Permisos para suscribirse y cancelar la suscripción a AWS Marketplace para su usuario de IAM.
- Comprensión de los requisitos de CPU y RAM para la instancia.
- Una pareja de claves para la instancia de EC2.

Pasos

1. Vaya a la "Página de BlueXP en AWS Marketplace"
2. En la página de Marketplace, selecciona **Continuar con la suscripción** y luego selecciona **Continuar con la configuración**.



3. Cambie cualquiera de las opciones predeterminadas y seleccione **Continuar para iniciar**.
4. En **Elegir acción**, selecciona **Iniciar a través de EC2** y luego selecciona **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**.

5. 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**: Dependiendo de la disponibilidad de la región, elija un tipo de instancia que cumpla con los requisitos de RAM y CPU (se recomienda T3.xlarge).
   - **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.

Se requieren algunas reglas más para configuraciones específicas.

"Ver reglas de grupos de seguridad para AWS".

- **Configurar almacenamiento**: Mantenga el tamaño predeterminado y el tipo de disco para el volumen raíz.

  Si desea habilitar el cifrado de Amazon EBS en el volumen raíz, seleccione **Avanzado**, expanda **Volumen 1**, seleccione **Cifrado** y, a continuación, elija una clave KMS.

- **Detalles avanzados**: En **perfil de instancia de IAM**, elija la función de IAM que incluye los permisos necesarios para el conector.
- **Resumen**: Revisa el resumen y selecciona **Iniciar Instancia**.

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

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

   https://ipaddress

7. Después de iniciar sesión, configure el conector:
   a. Especifique la cuenta BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y configurado con su cuenta BlueXP.

Abra un explorador web y vaya al "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Si tienes buckets de Amazon S3 en la misma cuenta de AWS en la que creaste el conector, verás que aparece automáticamente un entorno de trabajo de Amazon S3 en el lienzo de BlueXP. "Descubre cómo gestionar buckets S3 de BlueXP"

Instale manualmente el conector en AWS

Para instalar manualmente Connector en su propio host Linux, debe revisar los requisitos del host, configurar la red, preparar los permisos de AWS, instalar Connector y, a continuación, proporcionar los permisos que preparó.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Revise 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.

Host dedicado

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

Sistemas operativos compatibles

- Sistema operativo Ubuntu 22,04 LTS
- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7,6, 7,7, 7,8 y 7,9

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

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

Hipervisor

Se requiere un hipervisor con configuración básica o alojado certificado para ejecutar Ubuntu, CentOS o Red Hat Enterprise Linux.

"Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"

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.

Par de claves

Cuando cree el conector, deberá seleccionar un par de claves EC2 para utilizarlo con la instancia.

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 en el host antes de instalar Connector.

- La versión mínima admitida es 19,3.1.
- La versión máxima admitida es 25,0.5.

  "Ver las instrucciones de instalación"

Paso 2: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados durante la instalación manual

Al instalar manualmente el conector en su propio host Linux, el instalador del conector requiere acceso 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://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  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.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"

Puntos finales	Específico
https://support.netapp.com https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	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 de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Paso 3: Configurar permisos

Necesitas proporcionar permisos de AWS a BlueXP mediante una de las siguientes opciones:

- Opción 1: Crear políticas IAM y asociar las políticas a una función IAM que se puede asociar a la instancia de EC2.
- Opción 2: Proporcione a BlueXP la clave de acceso de AWS para un usuario de IAM que tenga los permisos requeridos.

Sigue los pasos para preparar permisos para BlueXP.

Rol IAM

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:
   a. Selecciona **Políticas > Crear política**.
   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".
   c. Finalice los pasos restantes para crear la directiva.

      Dependiendo de los servicios de BlueXP que tenga previsto utilizar, puede que necesite crear una segunda política. 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. "Obtenga más información sobre las políticas de IAM para el conector".
3. Cree un rol IAM:
   a. Selecciona **Roles > Crear rol**.
   b. Seleccione **Servicio AWS > EC2**.
   c. Agregue permisos asociando la directiva que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

Resultado

Ahora tiene la función IAM que puede asociar con la instancia de EC2 después de instalar el conector.

Clave de acceso de AWS

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:

   a. Selecciona **Políticas > Crear política**.
   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".
   c. Finalice los pasos restantes para crear la directiva.

      Dependiendo de los servicios de BlueXP que tenga previsto utilizar, puede que necesite crear una segunda política.

   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. "Obtenga más información sobre las políticas de IAM para el conector".
3. Adjunte las políticas a un usuario de IAM.
   - "Documentación de AWS: Crear roles de IAM"
   - "Documentación de AWS: Adición y eliminación de políticas de IAM"
4. Asegúrese de que el usuario tiene una clave de acceso que puede agregar a BlueXP después de instalar el conector.

Resultado

Ahora dispone de un usuario de IAM que tiene los permisos necesarios y una clave de acceso que puede

proporcionar a BlueXP.

Paso 4: Instale el conector

Una vez completados los requisitos previos, puede instalar manualmente el software en su propio host Linux.

Antes de empezar

Debe tener lo siguiente:

- 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.

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

  Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

- Un certificado firmado por CA, si el servidor proxy utiliza HTTPS o si el proxy es un proxy de interceptación.

Acerca de esta tarea

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 "en línea" del conector que se utiliza en su red o en la nube. Hay disponible un instalador "sin conexión" independiente para el conector, pero sólo es compatible con implementaciones en modo privado.

4. Asigne permisos para ejecutar el script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

5. Ejecute el script de instalación.

```
./BlueXP-Connector-Cloud-<version> --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:

```
./BlueXP-Connector-Cloud-v3.9.38 --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://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Tenga en cuenta lo siguiente:

  - El usuario puede ser un usuario local o un usuario de dominio.
  - Para un usuario de dominio, debe utilizar el código ASCII para \ como se muestra anteriormente.
  - BlueXP no admite contraseñas que incluyan el carácter @.

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

6. Espere a que finalice la instalación.

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

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

   https://ipaddress

8. Después de iniciar sesión, configure el conector:
   a. Especifique la cuenta BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.

c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

   Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y está configurado con su cuenta BlueXP.

Si tienes buckets de Amazon S3 en la misma cuenta de AWS en la que creaste el conector, verás que aparece automáticamente un entorno de trabajo de Amazon S3 en el lienzo de BlueXP. "Descubre cómo gestionar buckets S3 de BlueXP"

Paso 5: Proporcionar permisos a BlueXP

Ahora que ha instalado Connector, debe proporcionar a BlueXP los permisos de AWS que configuró anteriormente. Al proporcionar los permisos, BlueXP podrá gestionar tus datos y la infraestructura de almacenamiento en AWS.

Rol IAM

Conecte la función IAM que ha creado previamente a la instancia de Connector EC2.

Pasos

1. Vaya a la consola de Amazon EC2.
2. Seleccione **instancias**.
3. Seleccione la instancia de conector.
4. Seleccione **acciones > Seguridad > Modificar función IAM**.
5. Seleccione el rol de IAM y seleccione **Actualizar rol de IAM**.

Resultado

BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

Vaya a la "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Clave de acceso de AWS

Proporcione a BlueXP la clave de acceso de AWS para un usuario de IAM que tenga los permisos necesarios.

Pasos

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

3. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Servicios Web de Amazon > conector**.
   b. **Definir credenciales**: Introduzca una clave de acceso y una clave secreta de AWS.
   c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.
   d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

Vaya a la "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Azure

Opciones de instalación del conector en Azure

Hay varias formas diferentes de crear un conector en Azure. Directamente desde BlueXP es la forma más común.

Están disponibles las siguientes opciones de instalación:

- "Crea un conector directamente desde BlueXP" (esta es la opción estándar)

  Esta acción lanza una VM que ejecuta Linux y el software Connector en una vnet de su elección.

- "Cree un conector desde Azure Marketplace"

  Esta acción también inicia una máquina virtual que ejecuta Linux y el software Connector, pero la puesta en marcha se inicia directamente desde Azure Marketplace en lugar de desde BlueXP.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará a la forma en que se prepara para la instalación. Esto incluye cómo proporciona BlueXP los permisos necesarios para autenticar y gestionar recursos en Azure.

Cree un conector en Azure desde BlueXP

Para crear un conector en Azure desde BlueXP, debe configurar la red, preparar los permisos de Azure y, a continuación, crear el conector.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

Región de Azure

Si utiliza Cloud Volumes ONTAP, el conector debe desplegarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que gestiona, o en el "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"

Vnet y subred

Al crear el conector, debe especificar el vnet y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://support.netapp.com https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para actualizar el conector y sus componentes de Docker.

Extremos en los que se han contactado desde la consola de BlueXP

A medida que utiliza la consola basada en Web BlueXP que se proporciona a través de la capa SaaS, se pone en contacto con varios extremos para completar las tareas de gestión de datos. Esto incluye los extremos que se ponen en contacto para poner en marcha el conector desde la consola de BlueXP.

"Consulte la lista de extremos con los que se ha contactado desde la consola de BlueXP".

Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Crear un rol personalizado

Cree una función personalizada de Azure que pueda asignar a su cuenta de Azure o a un director de servicio de Microsoft Entra. BlueXP autentica con Azure y utiliza estos permisos para crear la instancia de Connector en su nombre.

Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

Pasos

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

   > Este rol personalizado 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/rea
d",
        "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/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/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.

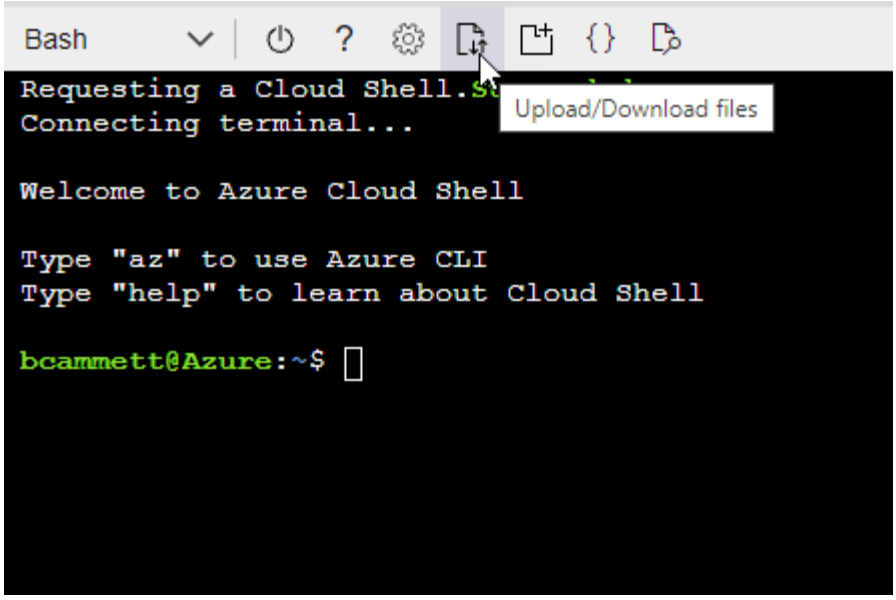
   ejemplo

```
"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*. Ahora puede aplicar esta función personalizada a su cuenta de usuario o a un director de servicio.

Paso 3: Configurar la autenticación

Al crear el conector desde BlueXP, debes proporcionar un inicio de sesión que permita a BlueXP autenticarse con Azure y poner en marcha la máquina virtual. Dispone de dos opciones:

1. Inicie sesión con su cuenta de Azure cuando se le solicite. Esta cuenta debe tener permisos de Azure específicos. Esta es la opción predeterminada.
2. Proporcionar detalles acerca de un director de servicio de Microsoft Entra. Este principal de servicio también requiere permisos específicos.

Sigue los pasos para preparar uno de estos métodos de autenticación para usarlos con BlueXP.

Cuenta de Azure

Asigne la función personalizada al usuario que implementará Connector desde BlueXP.

Pasos

1. En el portal de Azure, abra el servicio **Suscripciones** y seleccione la suscripción del usuario.
2. Haga clic en **Control de acceso (IAM)**.
3. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos:
   a. 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.

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

Resultado

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

Director de servicios

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

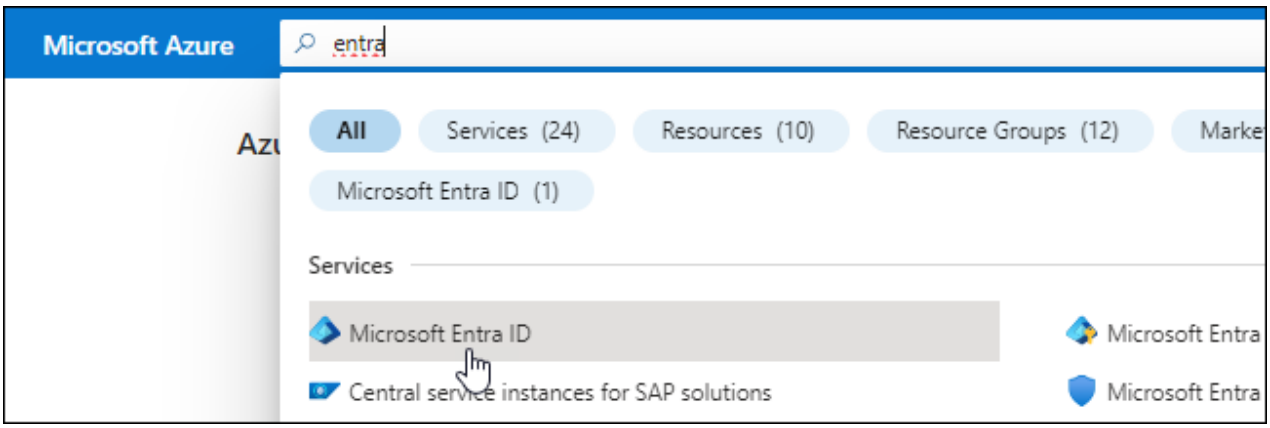
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

Cree una aplicación Microsoft Entra para el control de acceso basado en roles

1. Asegúrese de tener permisos en Azure para crear una aplicación de Active Directory y para asignar la aplicación a un rol.

   Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios"

2. Desde el portal de Azure, abra el servicio **Microsoft Entra ID**.



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. 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.
6. Seleccione **Registrar**.

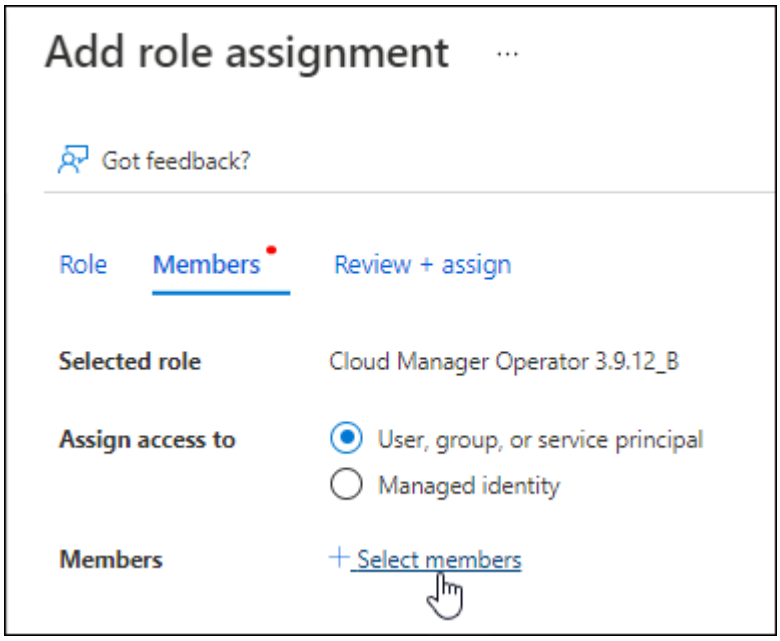
   Ha creado la aplicación AD y el director de servicio.

Asigne la función personalizada a la aplicación

1. En el portal de Azure, abra el servicio **Suscripciones**.
2. Seleccione la suscripción.
3. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
4. En la ficha **rol**, seleccione el rol **operador BlueXP** y haga clic en **Siguiente**.
5. En la ficha **Miembros**, realice los siguientes pasos:

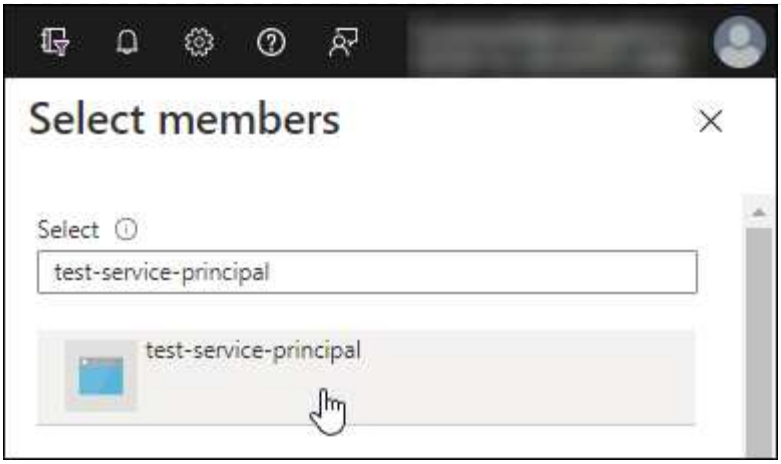
   a. Mantener seleccionado **Usuario, grupo o principal de servicio**.

   b. Haga clic en **Seleccionar miembros**.



   c. Busque el nombre de la aplicación.

   Veamos un ejemplo:



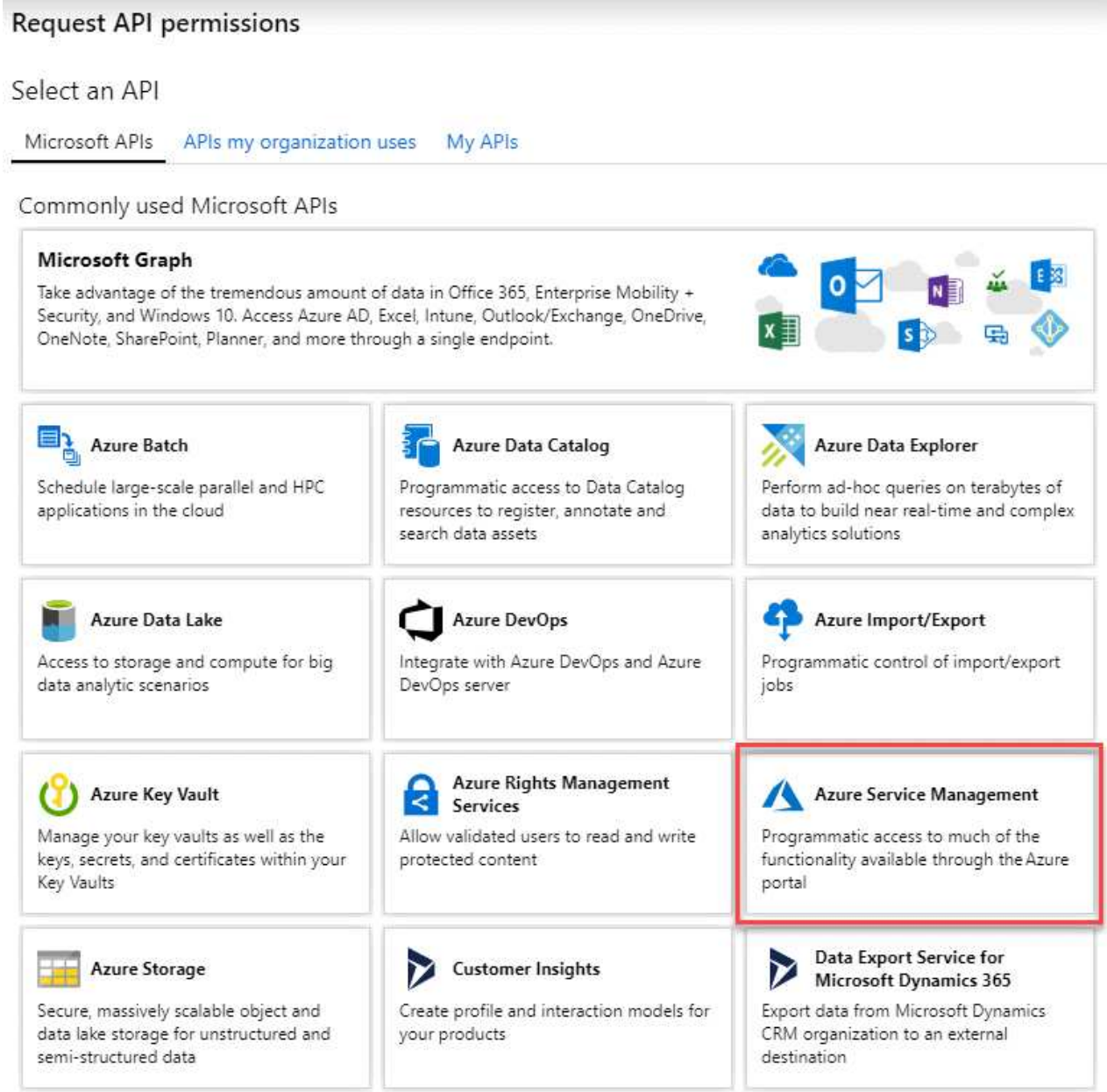
   a. Seleccione la aplicación y haga clic en **Seleccionar**.
   b. Haga clic en **Siguiente**.
6. Haga clic en **revisar + asignar**.

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

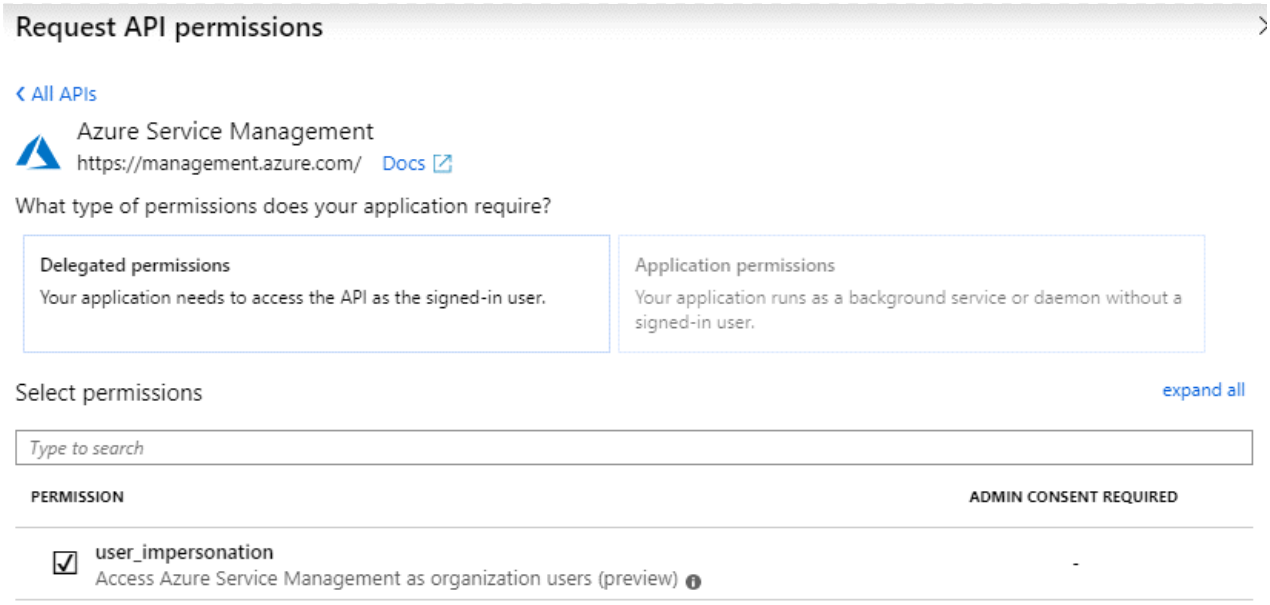
   Si desea administrar recursos en varias suscripciones de Azure, debe vincular el principal de servicio a cada una de esas suscripciones. Por ejemplo, BlueXP te permite seleccionar la suscripción que desees utilizar al implementar Cloud Volumes ONTAP.

Añada permisos de API de administración de servicios de Windows Azure

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Seleccione **permisos de API > Agregar un permiso**.
3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.

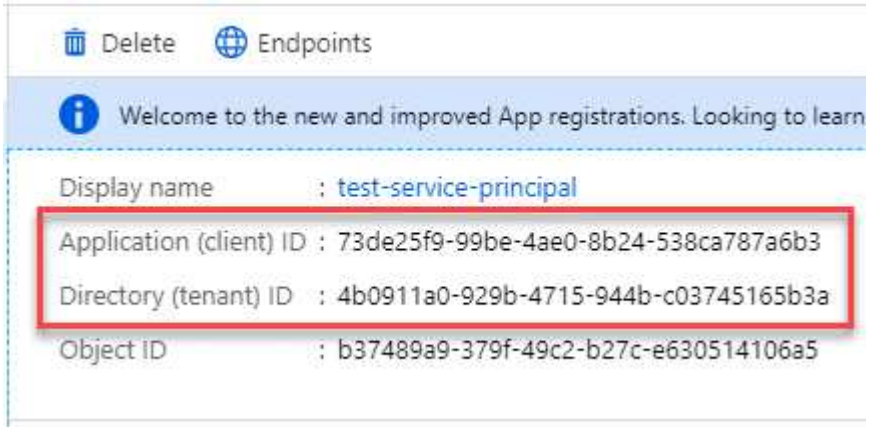


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



Obtenga el ID de aplicación y el ID de directorio de la aplicación

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Cree un secreto de cliente

1. Abra el servicio **Microsoft Entra ID**.
2. Seleccione **App registres** y seleccione su aplicación.
3. Seleccione **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copie el valor del secreto de cliente.

Ahora tienes un secreto de cliente que BlueXP puede usarlo para autenticar con Microsoft Entra ID.

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.

Paso 4: Crear el conector

Crea el Connector directamente desde la consola basada en web de BlueXP.

Acerca de esta tarea

Al crear el conector desde BlueXP se implementa una máquina virtual en Azure con una configuración predeterminada. Después de crear el conector, no debe cambiar a un tipo de máquina virtual más pequeño que tenga menos CPU o RAM. "Obtenga información sobre la configuración predeterminada para el conector".

Antes de empezar

Debe tener lo siguiente:

- 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
- Una clave pública SSH, si desea utilizar ese método de autenticación para la máquina virtual Connector. La otra opción para el método de autenticación es usar una contraseña.

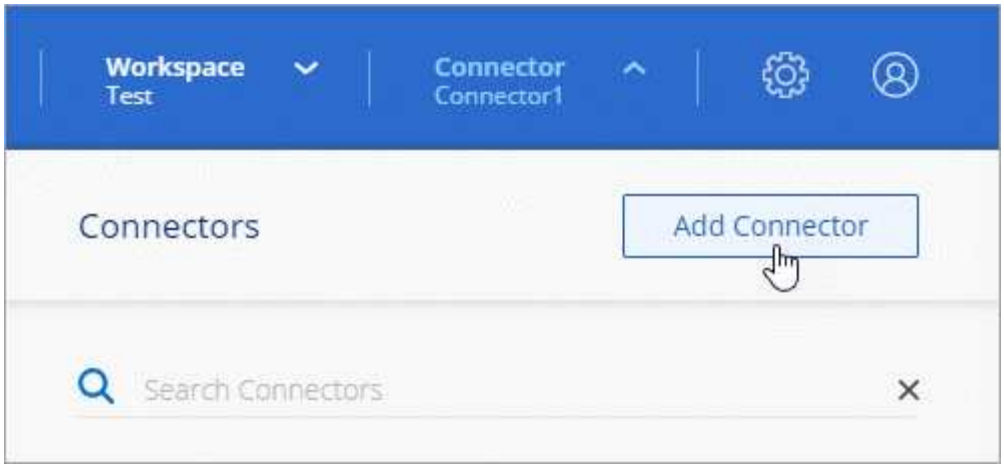
  "Obtenga más información sobre cómo conectarse a una máquina virtual de Linux en Azure"

- 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 configurado anteriormente para implementar la VM de Connector.

Pasos

1. Seleccione la lista desplegable **Connector** y seleccione **Add Connector**.



2. Elija **Microsoft Azure** como proveedor de cloud.
3. En la página **despliegue de un conector**:

   a. En **autenticación**, seleccione la opción de autenticación que coincida con la forma en que configuró los permisos de Azure:

      - Seleccione **cuenta de usuario de Azure** para iniciar sesión en su cuenta de Microsoft, que debería tener los permisos necesarios.

        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.

      - Seleccione **Active Directory Service principal** para introducir información sobre el principal de servicio de Microsoft Entra que otorga los permisos necesarios:
        - ID de aplicación (cliente)
        - ID de directorio (inquilino)
        - Secreto de cliente

   Aprenda cómo obtener estos valores para un director de servicio.

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 para la máquina virtual Connector que está creando.

     El método de autenticación para la máquina virtual puede ser una contraseña o una clave pública SSH.

   "Obtenga más información sobre cómo conectarse a una máquina virtual de Linux en Azure"

   - **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 de Azure asociadas a este rol. Cada suscripción que elija proporciona los permisos de Connector para administrar los recursos de esa suscripción (por ejemplo, Cloud Volumes ONTAP).

- **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 las reglas entrantes y salientes requeridas.

  "Ver reglas de grupo de seguridad para Azure".

- **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.

Resultado

Una vez completado el proceso, el conector está disponible para su uso en BlueXP.

Si tienes almacenamiento de Azure Blob en la misma suscripción de Azure donde creaste el conector, verás que aparece automáticamente un entorno de trabajo de almacenamiento de Azure Blob en el lienzo de BlueXP. "Descubre cómo gestionar el almacenamiento de Azure Blob desde BlueXP"

Cree un conector desde Azure Marketplace

Para crear un conector desde Azure Marketplace, debe configurar su red, preparar los permisos de Azure, revisar los requisitos de la instancia y, a continuación, crear el conector.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

Región de Azure

Si utiliza Cloud Volumes ONTAP, el conector debe desplegarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que gestiona, o en el "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"

Vnet y subred

Al crear el conector, debe especificar el vnet y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://support.netapp.com https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	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 de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Revise los requisitos de VM

Al crear el conector, debe elegir un tipo de máquina virtual que cumpla los siguientes requisitos.

CPU

4 núcleos o 4 vCPU

RAM

14 GB

Tamaño de la máquina virtual de Azure

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

Paso 3: Configurar permisos

Puede proporcionar permisos de las siguientes maneras:

- Opción 1: Asigne un rol personalizado a la máquina virtual de Azure mediante una identidad gestionada asignada por el sistema.
- Opción 2: Proporcione a BlueXP las credenciales de una entidad de servicio de Azure que tenga los permisos necesarios.

Sigue estos pasos para configurar permisos para BlueXP.

Función personalizada

Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

Pasos

1. Si tiene pensado instalar manualmente el software en su propio host, habilite una identidad gestionada asignada por el sistema en la máquina virtual para poder ofrecer los permisos de Azure necesarios a través de un rol personalizado.

   "Documentación de Microsoft Azure: Configure las identidades gestionadas para los recursos de Azure en una máquina virtual mediante el portal de Azure"

2. Copie el contenido de "Permisos de función personalizada para el conector" Y guárdelos en un archivo JSON.
3. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

   Debes añadir el ID de cada suscripción de Azure que quieras utilizar con BlueXP.

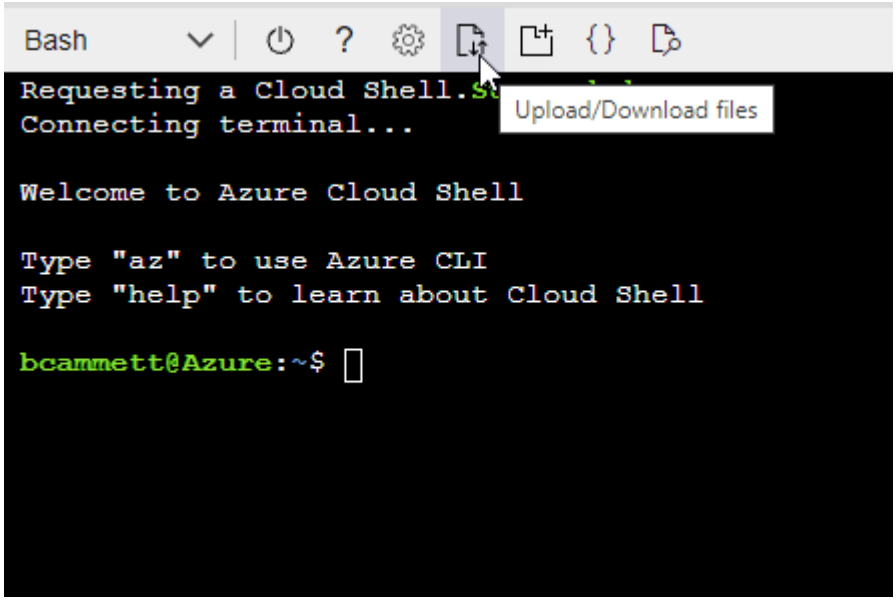
   ejemplo

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

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

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

Resultado

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

Director de servicios

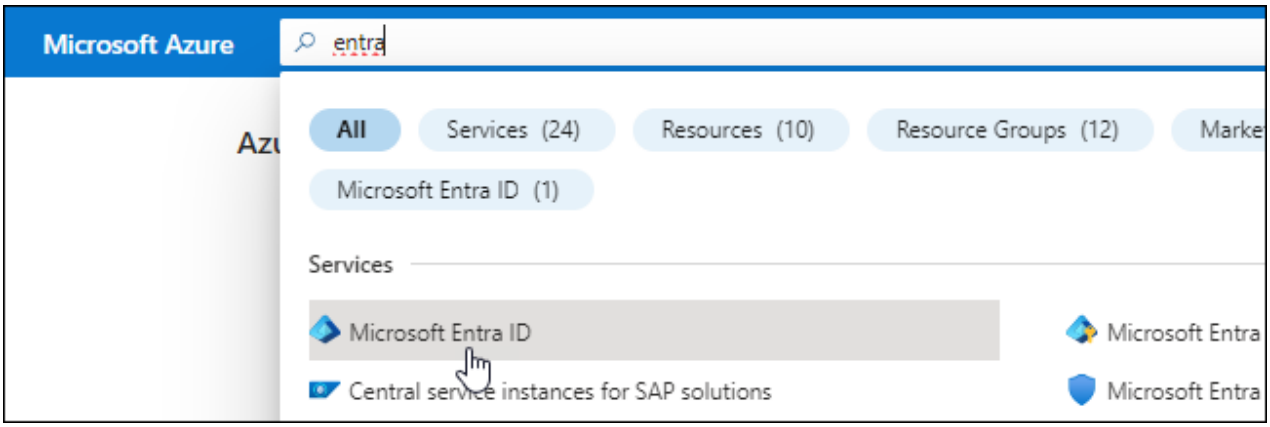
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

Cree una aplicación Microsoft Entra para el control de acceso basado en roles

1. Asegúrese de tener permisos en Azure para crear una aplicación de Active Directory y para asignar la aplicación a un rol.

   Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios"

2. Desde el portal de Azure, abra el servicio **Microsoft Entra ID**.



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. 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.
6. Seleccione **Registrar**.

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la

CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

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.

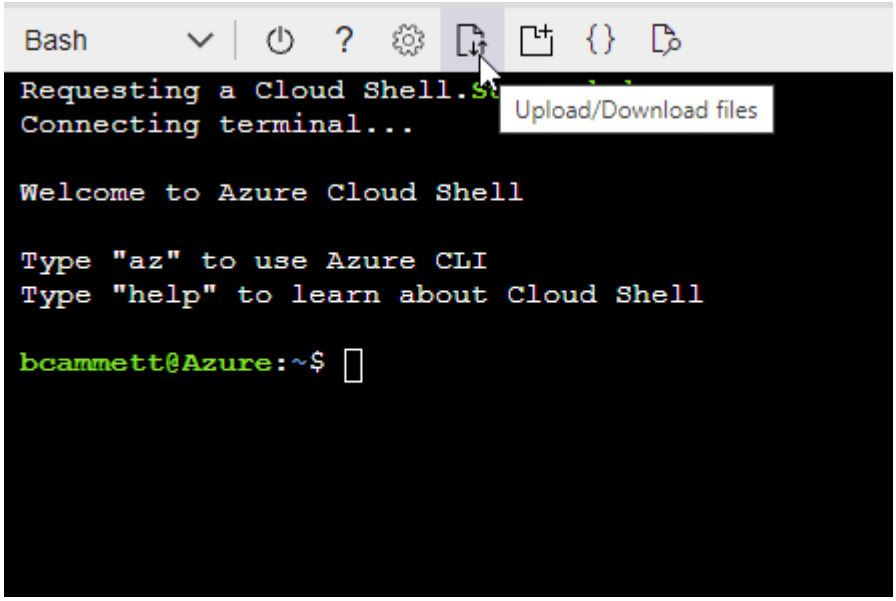
   ejemplo

```
"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:

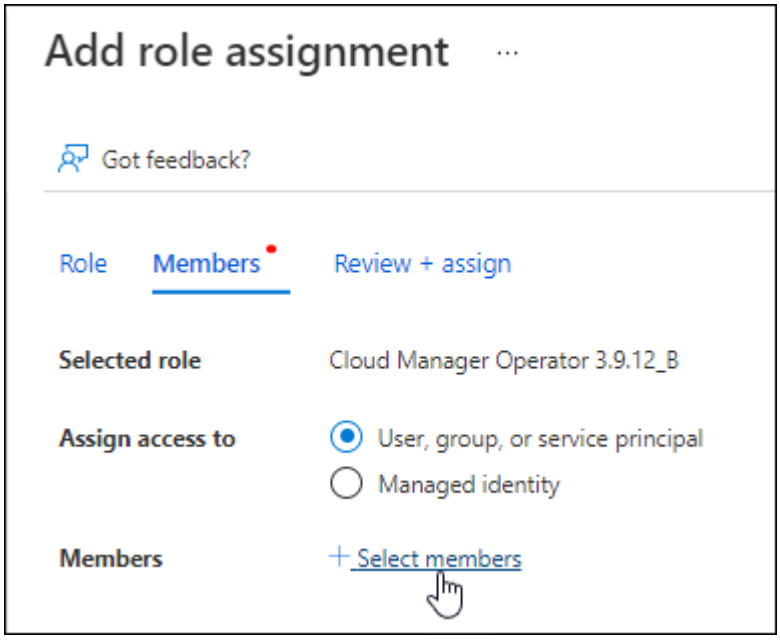
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

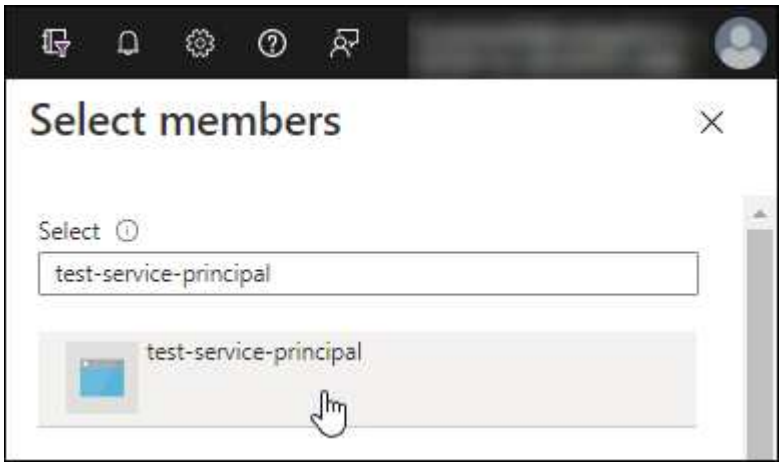
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**, realice los siguientes pasos:

      - Mantener seleccionado **Usuario, grupo o principal de servicio**.
      - Seleccione **Seleccionar miembros**.



      - Busque el nombre de la aplicación.

        Veamos un ejemplo:



      - Seleccione la aplicación y seleccione **Seleccionar**.
      - Seleccione **Siguiente**.

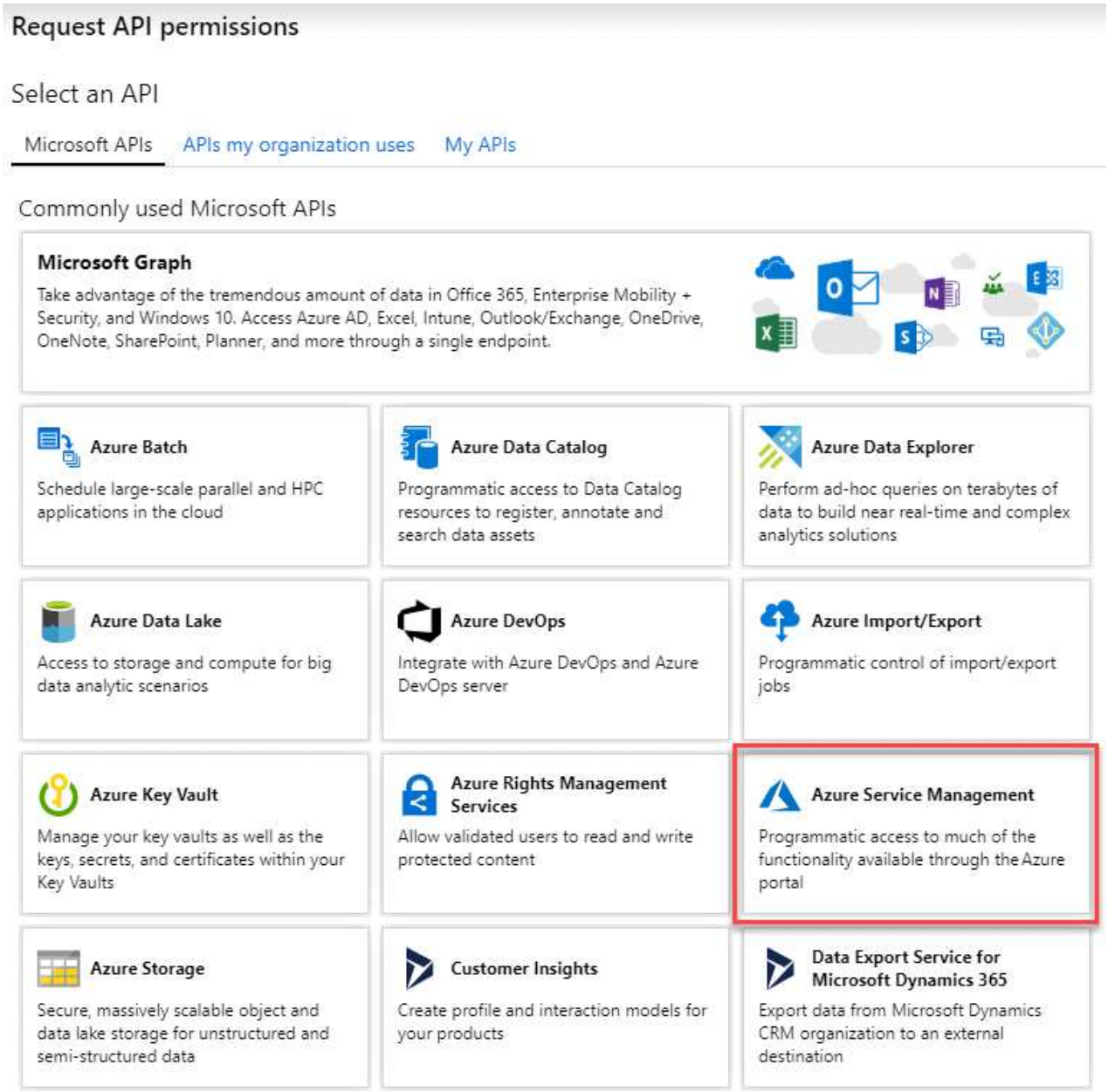
f. Seleccione **revisar + asignar**.

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

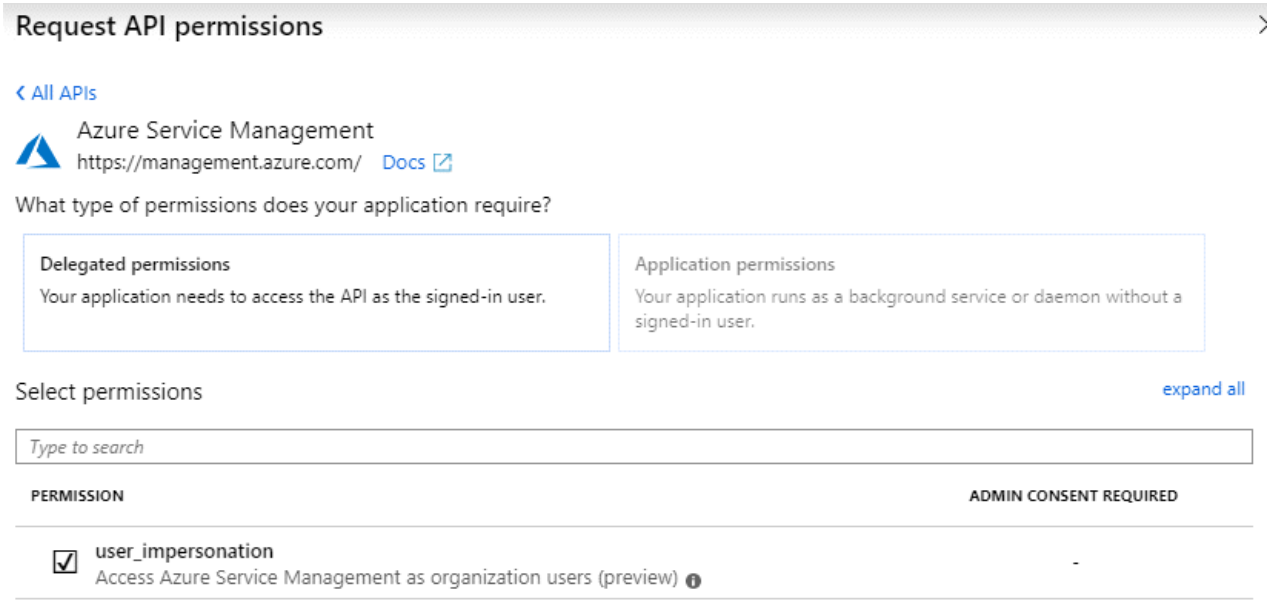
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. BlueXP le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

Añada permisos de API de administración de servicios de Windows Azure

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Seleccione **permisos de API > Agregar un permiso**.
3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.

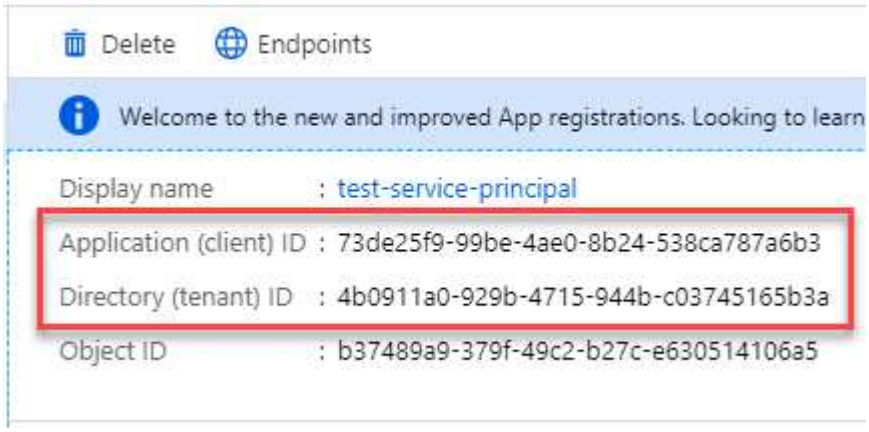


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



Obtenga el ID de aplicación y el ID de directorio de la aplicación

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Cree un secreto de cliente

1. Abra el servicio **Microsoft Entra ID**.
2. Seleccione **App registres** y seleccione su aplicación.
3. Seleccione **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copie el valor del secreto de cliente.

Ahora tienes un secreto de cliente que BlueXP puede usarlo para autenticar con Microsoft Entra ID.

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.

Paso 4: Crear el conector

Inicie Connector directamente desde Azure Marketplace.

Acerca de esta tarea

Al crear el conector desde Azure Marketplace se implementa una máquina virtual en Azure con una configuración predeterminada. "Obtenga información sobre la configuración predeterminada para el conector".

Antes de empezar

Debe tener lo siguiente:

- 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
- Una clave pública SSH, si desea utilizar ese método de autenticación para la máquina virtual Connector. La otra opción para el método de autenticación es usar una contraseña.

  "Obtenga más información sobre cómo conectarse a una máquina virtual de Linux en Azure"

- 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 configurado anteriormente para implementar la VM de Connector.

Pasos

1. Vaya a la página NetApp Connector VM del Azure Marketplace.

   "Página de Azure Marketplace para regiones comerciales"

2. Selecciona **Obtenlo ahora** y luego selecciona **Continuar**.
3. Desde el portal de Azure, seleccione **Crear** y siga los pasos para configurar la máquina virtual.

   Tenga en cuenta lo siguiente al configurar la máquina virtual:

   - **VM size**: Elija un tamaño de VM que cumpla con los requisitos de CPU y RAM. Recomendamos DS3 v2.
   - **Discos**: El conector puede funcionar de forma óptima con discos HDD o SSD.
   - **Grupo de seguridad de red**: El conector requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

     "Ver reglas de grupo de seguridad para Azure".

   - **Identidad**: En **Gestión**, seleccione **Activar identidad administrada asignada por el sistema**.

     Esta configuración es importante porque una identidad administrada permite que la máquina virtual Connector se identifique con Microsoft Entra ID sin proporcionar credenciales. "Obtenga más información sobre las identidades gestionadas para recursos de Azure".

4. En la página **Review + create**, revise sus selecciones y seleccione **Create** 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 BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y está configurado con su cuenta BlueXP.

Si tienes almacenamiento de Azure Blob en la misma suscripción de Azure donde creaste el conector, verás que aparece automáticamente un entorno de trabajo de almacenamiento de Azure Blob en el lienzo de BlueXP. "Descubre cómo gestionar el almacenamiento de Azure Blob desde BlueXP"

Paso 5: Proporcionar permisos a BlueXP

Ahora que has creado Connector, debes proporcionar a BlueXP los permisos que configuraste anteriormente. Al proporcionar los permisos, BlueXP podrá gestionar sus datos y la infraestructura de almacenamiento en

Azure.

Función personalizada

Vaya al portal de Azure y asigne el rol personalizado de Azure a la máquina virtual Connector para una o más suscripciones.

Pasos

1. En el Portal de Azure, abra el servicio **Suscripciones** y seleccione su suscripción.

   Es importante asignar el rol desde el servicio **Suscripciones** porque especifica el alcance de la asignación de rol en el nivel de suscripción. El *scope* define el juego de recursos al que se aplica el acceso. Si especifica un ámbito a otro nivel (por ejemplo, a nivel de máquina virtual), se verá afectada su capacidad para completar acciones desde BlueXP.

   "Documentación de Microsoft Azure: Conozca el ámbito de control de acceso basado en roles de Azure"

2. Selecciona **Control de acceso (IAM)** > **Añadir** > **Añadir asignación de rol**.
3. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **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.

4. En la ficha **Miembros**, realice los siguientes pasos:
   a. Asignar acceso a una **identidad administrada**.
   b. Seleccione **Seleccionar miembros**, seleccione la suscripción en la que se creó la máquina virtual Connector, en **Identidad administrada**, elija **Máquina virtual** y, a continuación, seleccione la máquina virtual Connector.
   c. Selecciona **Seleccionar**.
   d. Seleccione **Siguiente**.
   e. Seleccione **revisar + asignar**.
   f. Si desea administrar recursos en suscripciones adicionales de Azure, cambie a esa suscripción y repita estos pasos.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

El futuro

Vaya a la "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Director de servicios

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.

a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.

b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:

   - ID de aplicación (cliente)
   - ID de directorio (inquilino)
   - Secreto de cliente

c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Instale manualmente el conector en Azure

Para instalar manualmente Connector en su propio host Linux, debe revisar los requisitos del host, configurar la red, preparar los permisos de Azure, instalar Connector y, a continuación, proporcionar los permisos preparados.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Revise 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.

Host dedicado

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

Sistemas operativos compatibles

- Sistema operativo Ubuntu 22,04 LTS
- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7,6, 7,7, 7,8 y 7,9

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

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

Hipervisor

Se requiere un hipervisor con configuración básica o alojado certificado para ejecutar Ubuntu, CentOS o Red Hat Enterprise Linux.

"Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"

CPU

4 núcleos o 4 vCPU

RAM

14 GB

Tamaño de la máquina virtual de Azure

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

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 en el host antes de instalar Connector.

- La versión mínima admitida es 19,3.1.
- La versión máxima admitida es 25,0.5.

"Ver las instrucciones de instalación"

Paso 2: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

Región de Azure

Si utiliza Cloud Volumes ONTAP, el conector debe desplegarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que gestiona, o en el "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"

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados durante la instalación manual

Al instalar manualmente el conector en su propio host Linux, el instalador del conector requiere acceso 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://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  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.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://support.netapp.com https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	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 de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Paso 3: Configurar permisos

Necesitas proporcionar permisos de Azure a BlueXP mediante una de las siguientes opciones:

- Opción 1: Asigne un rol personalizado a la máquina virtual de Azure mediante una identidad gestionada asignada por el sistema.
- Opción 2: Proporcione a BlueXP las credenciales de una entidad de servicio de Azure que tenga los permisos necesarios.

Sigue los pasos para preparar permisos para BlueXP.

Función personalizada

Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

Pasos

1. Si tiene pensado instalar manualmente el software en su propio host, habilite una identidad gestionada asignada por el sistema en la máquina virtual para poder ofrecer los permisos de Azure necesarios a través de un rol personalizado.

   "Documentación de Microsoft Azure: Configure las identidades gestionadas para los recursos de Azure en una máquina virtual mediante el portal de Azure"

2. Copie el contenido de "Permisos de función personalizada para el conector" Y guárdelos en un archivo JSON.
3. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

   Debes añadir el ID de cada suscripción de Azure que quieras utilizar con BlueXP.

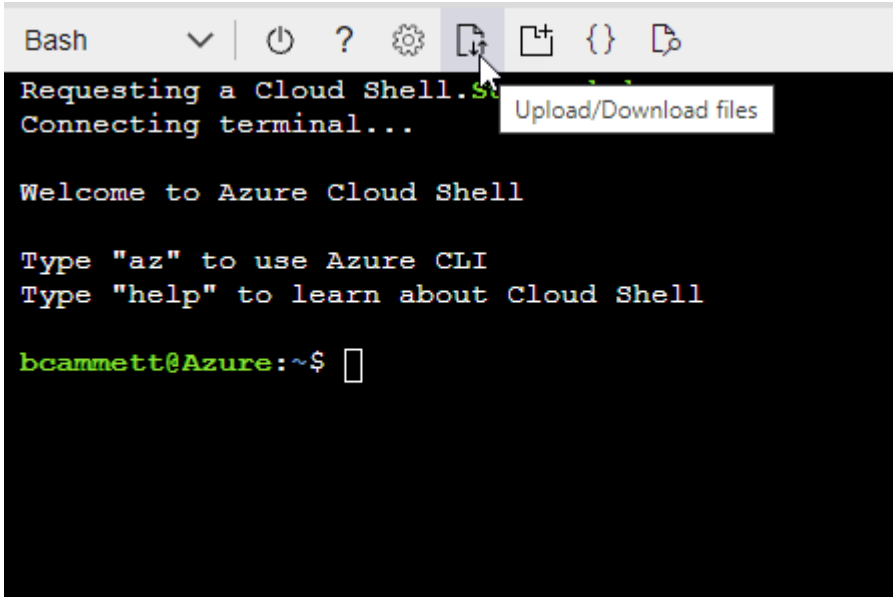
   ejemplo

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

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

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

Resultado

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

Director de servicios

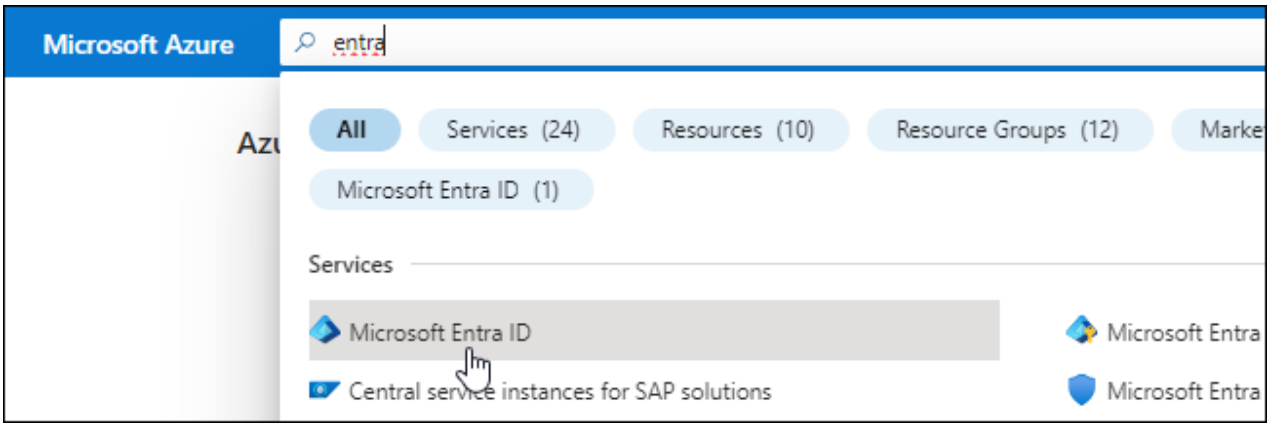
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

Cree una aplicación Microsoft Entra para el control de acceso basado en roles

1. Asegúrese de tener permisos en Azure para crear una aplicación de Active Directory y para asignar la aplicación a un rol.

   Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios"

2. Desde el portal de Azure, abra el servicio **Microsoft Entra ID**.



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. 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.
6. Seleccione **Registrar**.

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la

CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

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.

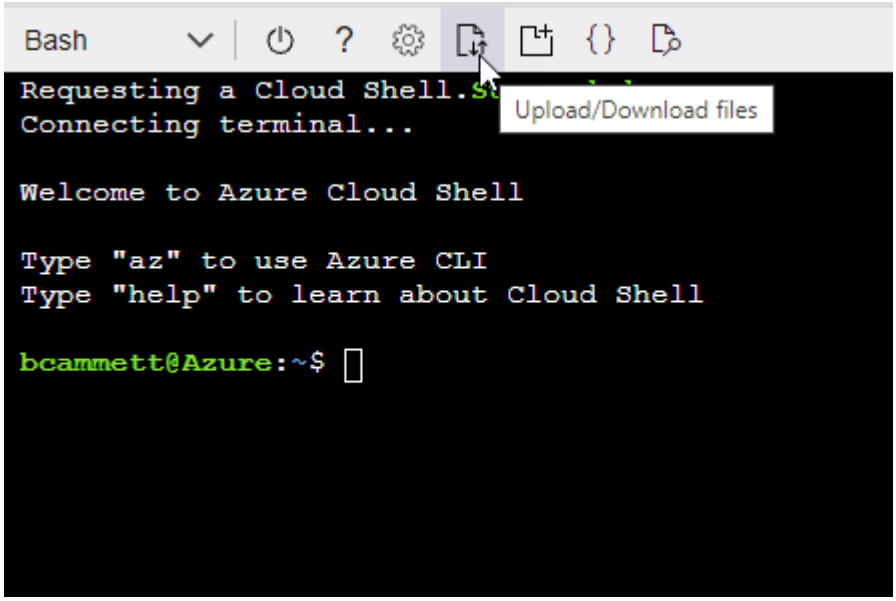
   ejemplo

```
"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:

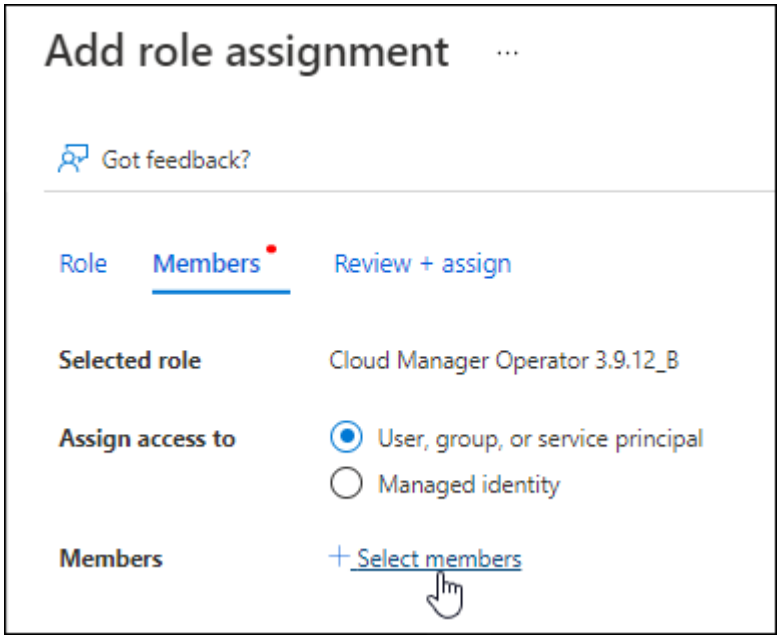
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

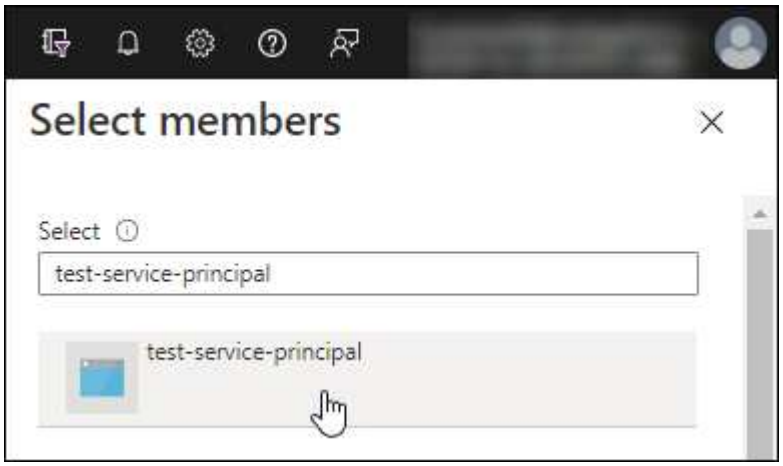
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**, realice los siguientes pasos:

      - Mantener seleccionado **Usuario, grupo o principal de servicio**.
      - Seleccione **Seleccionar miembros**.



      - Busque el nombre de la aplicación.

        Veamos un ejemplo:



      - Seleccione la aplicación y seleccione **Seleccionar**.
      - Seleccione **Siguiente**.

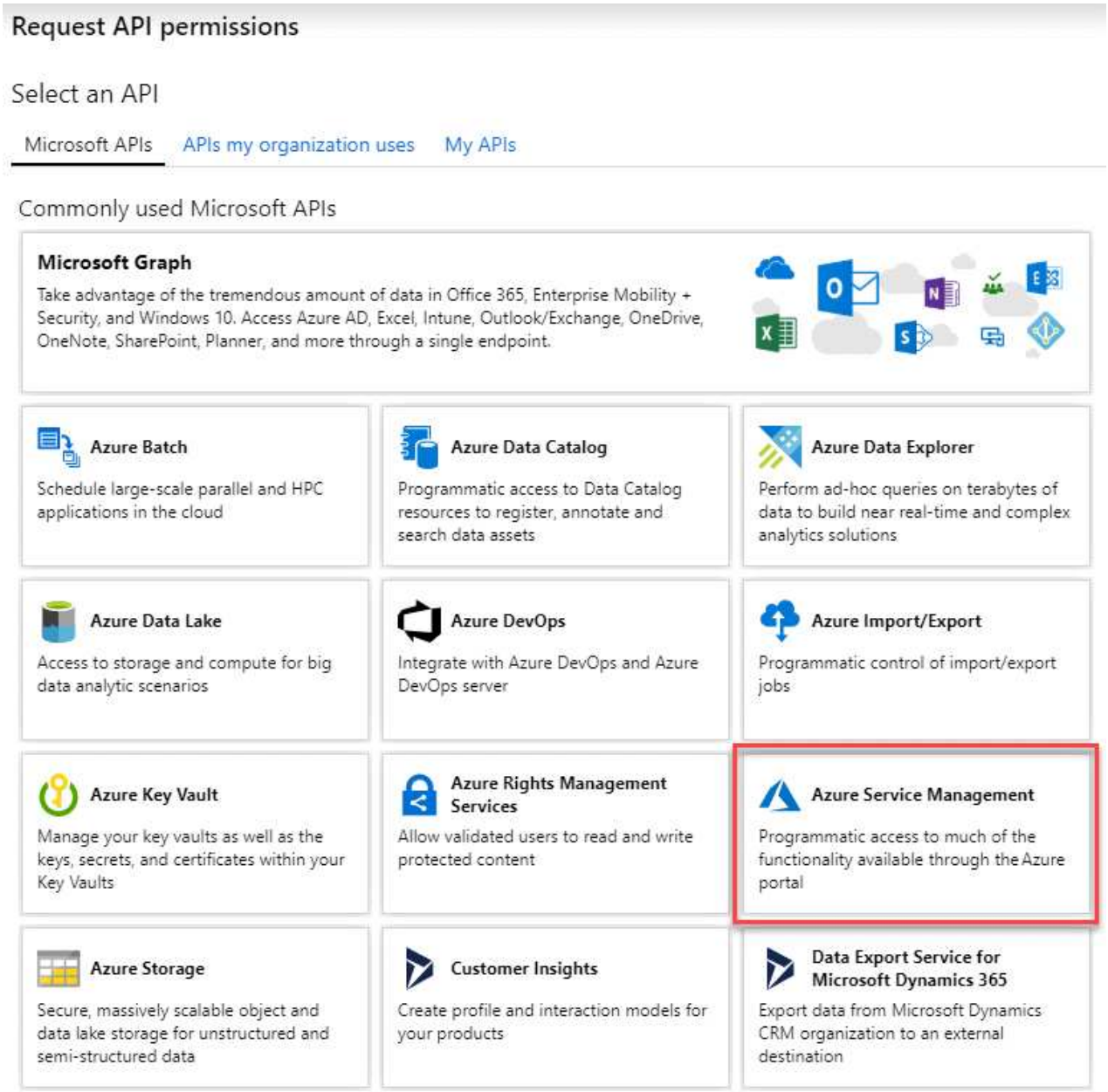
f. Seleccione **revisar + asignar**.

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

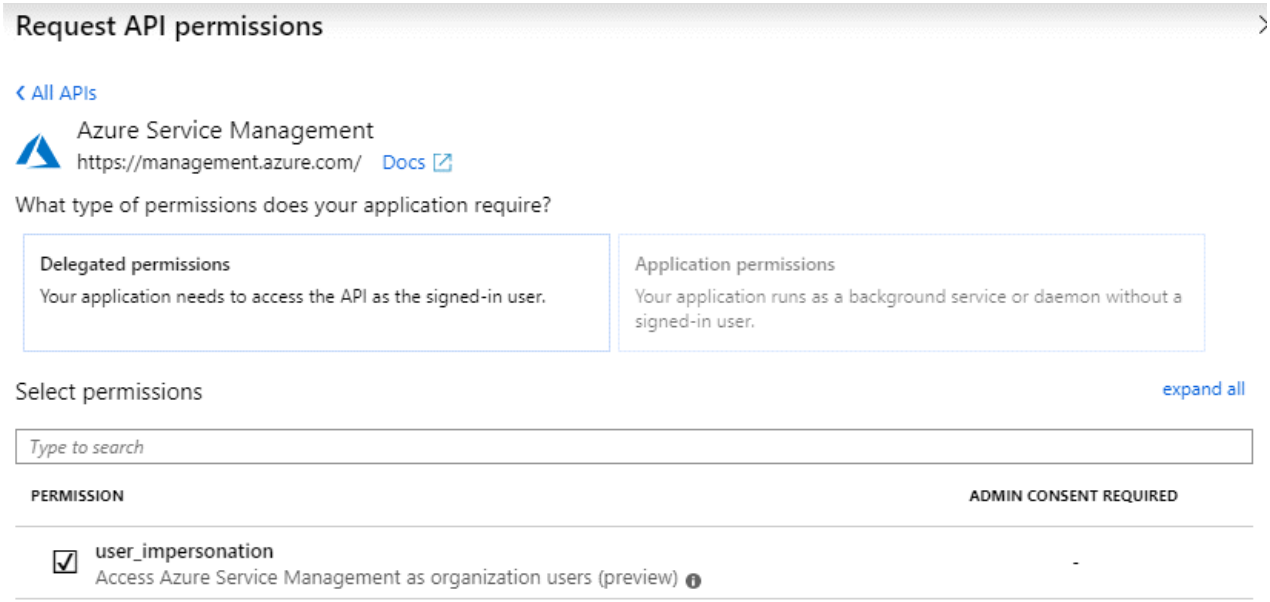
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. BlueXP le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

Añada permisos de API de administración de servicios de Windows Azure

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Seleccione **permisos de API > Agregar un permiso**.
3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.

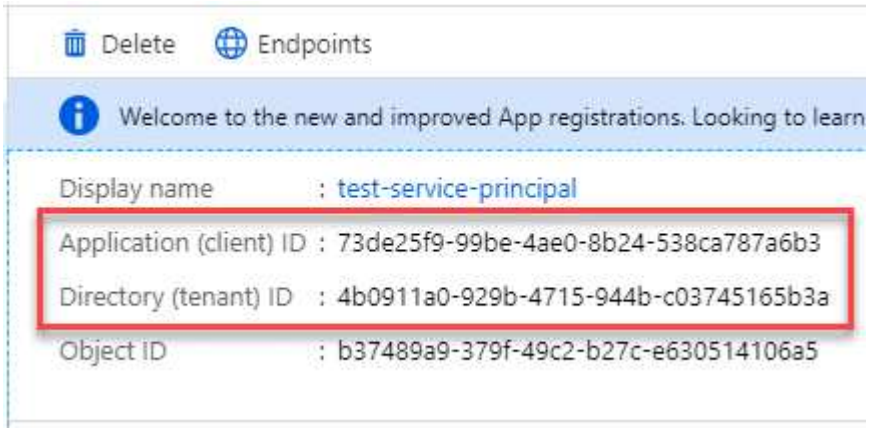


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



Obtenga el ID de aplicación y el ID de directorio de la aplicación

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Cree un secreto de cliente

1. Abra el servicio **Microsoft Entra ID**.
2. Seleccione **App registres** y seleccione su aplicación.
3. Seleccione **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copie el valor del secreto de cliente.

Ahora tienes un secreto de cliente que BlueXP puede usarlo para autenticar con Microsoft Entra ID.

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.

Paso 4: Instale el conector

Una vez completados los requisitos previos, puede instalar manualmente el software en su propio host Linux.

Antes de empezar

Debe tener lo siguiente:

- 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.

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

  Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

- Un certificado firmado por CA, si el servidor proxy utiliza HTTPS o si el proxy es un proxy de interceptación.
- Una identidad gestionada habilitada en la máquina virtual de Azure para poder proporcionar los permisos de Azure necesarios a través de un rol personalizado.

  "Documentación de Microsoft Azure: Configure las identidades gestionadas para los recursos de Azure en una máquina virtual mediante el portal de Azure"

Acerca de esta tarea

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 "en línea" del conector que se utiliza en su red o en la nube. Hay disponible un instalador "sin conexión" independiente para el conector, pero sólo es compatible con implementaciones en modo privado.

4. Asigne permisos para ejecutar el script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Ejecute el script de instalación.

```
 ./BlueXP-Connector-Cloud-<version> --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:

```
 ./BlueXP-Connector-Cloud-v3.9.38 --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://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Tenga en cuenta lo siguiente:

     - El usuario puede ser un usuario local o un usuario de dominio.

- Para un usuario de dominio, debe utilizar el código ASCII para \ como se muestra anteriormente.
- BlueXP no admite contraseñas que incluyan el carácter @.

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

6. Espere a que finalice la instalación.

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

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

   https://ipaddress

8. Después de iniciar sesión, configure el conector:
   a. Especifique la cuenta BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y está configurado con su cuenta BlueXP.

Si tienes almacenamiento de Azure Blob en la misma suscripción de Azure donde creaste el conector, verás que aparece automáticamente un entorno de trabajo de almacenamiento de Azure Blob en el lienzo de BlueXP. "Descubre cómo gestionar el almacenamiento de Azure Blob desde BlueXP"

Paso 5: Proporcionar permisos a BlueXP

Ahora que ha instalado Connector, debe proporcionar a BlueXP los permisos de Azure que configuró anteriormente. Al proporcionar los permisos, BlueXP podrá gestionar sus datos y la infraestructura de almacenamiento en Azure.

Función personalizada

Vaya al portal de Azure y asigne el rol personalizado de Azure a la máquina virtual Connector para una o más suscripciones.

Pasos

1. En el Portal de Azure, abra el servicio **Suscripciones** y seleccione su suscripción.

   Es importante asignar el rol desde el servicio **Suscripciones** porque especifica el alcance de la asignación de rol en el nivel de suscripción. El *scope* define el juego de recursos al que se aplica el acceso. Si especifica un ámbito a otro nivel (por ejemplo, a nivel de máquina virtual), se verá afectada su capacidad para completar acciones desde BlueXP.

   "Documentación de Microsoft Azure: Conozca el ámbito de control de acceso basado en roles de Azure"

2. Selecciona **Control de acceso (IAM)** > **Añadir** > **Añadir asignación de rol**.
3. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **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.

4. En la ficha **Miembros**, realice los siguientes pasos:
   a. Asignar acceso a una **identidad administrada**.
   b. Seleccione **Seleccionar miembros**, seleccione la suscripción en la que se creó la máquina virtual Connector, en **Identidad administrada**, elija **Máquina virtual** y, a continuación, seleccione la máquina virtual Connector.
   c. Selecciona **Seleccionar**.
   d. Seleccione **Siguiente**.
   e. Seleccione **revisar + asignar**.
   f. Si desea administrar recursos en suscripciones adicionales de Azure, cambie a esa suscripción y repita estos pasos.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

El futuro

Vaya a la "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Director de servicios

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.

a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.

b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:

   - ID de aplicación (cliente)
   - ID de directorio (inquilino)
   - Secreto de cliente

c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Google Cloud

Opciones de instalación del conector en Google Cloud

Hay varias formas diferentes de crear un conector en Google Cloud. Directamente desde BlueXP es la forma más común.

Están disponibles las siguientes opciones de instalación:

- "Crea el conector directamente desde BlueXP" (esta es la opción estándar)

  Esta acción inicia una instancia de máquina virtual que ejecuta Linux y el software Connector en un VPC de su elección.

- "Cree el conector con gcloud"

  Esta acción también inicia una instancia de máquina virtual que ejecuta Linux y el software Connector, pero la puesta en marcha se inicia directamente desde Google Cloud en lugar de desde BlueXP.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará a la forma en que se prepara para la instalación. Esto incluye cómo proporciona BlueXP los permisos necesarios para autenticar y administrar recursos en Google Cloud.

Crea un conector en Google Cloud desde BlueXP o gcloud

Para crear un conector en Google Cloud desde BlueXP o mediante gcloud, debes configurar tu red, preparar permisos de Google Cloud, habilitar las API de Google Cloud y, a continuación, crear el conector.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Configurar redes

Configure su red para que Connector pueda gestionar recursos y procesos en su entorno de cloud híbrido. Por ejemplo, debe asegurarse de que las conexiones estén disponibles para las redes de destino y de que el

acceso a Internet de salida esté disponible.

VPC y subred

Al crear el conector, es necesario especificar el VPC y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://www.googleapis.com/compute/v1/ https://compute.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 https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para actualizar el conector y sus componentes de Docker.

Extremos en los que se han contactado desde la consola de BlueXP

A medida que utiliza la consola basada en Web BlueXP que se proporciona a través de la capa SaaS, se pone en contacto con varios extremos para completar las tareas de gestión de datos. Esto incluye los extremos que se ponen en contacto para poner en marcha el conector desde la consola de BlueXP.

"Consulte la lista de extremos con los que se ha contactado desde la consola de BlueXP".

Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Configure permisos para crear el conector

Antes de poder implementar un conector desde BlueXP o mediante gcloud, debes configurar permisos para el usuario de Google Cloud que implementará la máquina virtual de Connector.

Pasos

1. Cree un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya los siguientes permisos:

```yaml
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
```

b. Desde Google Cloud, active Cloud Shell.

c. Cargue el archivo YAML que incluya los permisos necesarios.

d. Cree un rol personalizado mediante `gcloud iam roles create` comando.

En el ejemplo siguiente se crea un rol denominado "connectorDeployment" en el nivel de proyecto:

Los roles de gcloud iam crean connectorDeployment --project=myproject --file=Connector -deployment.yaml

"Documentos de Google Cloud: Creación y gestión de roles personalizados"

2. Asigne esta función personalizada al usuario que implementará Connector desde BlueXP o mediante gcloud.

"Google Cloud docs: Conceda un único rol"

Resultado

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

Paso 3: Configurar permisos para el conector

Se necesita una cuenta de servicio de Google Cloud para proporcionar al Connector los permisos que BlueXP necesita para gestionar recursos en Google Cloud. Cuando cree el Connector, deberá asociar esta cuenta de servicio con la VM de Connector.

Pasos

1. Cree un rol personalizado en Google Cloud:

a. Cree un archivo YAML que incluya el contenido de "Permisos de cuenta de servicio para el conector".

b. Desde Google Cloud, active Cloud Shell.

c. Cargue el archivo YAML que incluya los permisos necesarios.

d. Cree un rol personalizado mediante `gcloud iam roles create` comando.

En el ejemplo siguiente se crea una función denominada "conector" en el nivel de proyecto:

```
gcloud iam roles create connector --project=myproject --file=connector.yaml
```

"Documentos de Google Cloud: Creación y gestión de roles personalizados"

2. Cree una cuenta de servicio en Google Cloud y asígnele el rol a la cuenta de servicio:
   a. En el servicio IAM y Admin, selecciona **Cuentas de servicio > Crear cuenta de servicio**.
   b. Ingrese los detalles de la cuenta de servicio y seleccione **Crear y continuar**.
   c. Seleccione la función que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

      "Documentos de Google Cloud: Crear una cuenta de servicio"

3. 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.

   a. En el servicio IAM & Admin, seleccione el proyecto de Google Cloud en el que desea crear sistemas Cloud Volumes ONTAP.
   b. 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.
      - Seleccione **Guardar**.

   Para obtener información detallada, consulte "Documentación de Google Cloud"

Resultado

Se ha configurado la cuenta de servicio del conector VM.

Paso 4: Configurar permisos de VPC compartidos

Si utiliza un VPC compartido para implementar recursos en un proyecto de servicio, tendrá que preparar los permisos.

Esta tabla es de referencia y el entorno debe reflejar la tabla de permisos cuando se haya completado la configuración de IAM.

Ver permisos de VPC compartidos

Identidad	Creador	Alojadas en	Permisos de proyecto de servicio	Permisos del proyecto host	Específico
Cuenta de Google para desplegar el conector	Personalizado	Proyecto de servicio	"Política de despliegue de conectores"	compute.networkUser	Despliegue del conector en el proyecto de servicio
Cuenta de servicio del conector	Personalizado	Proyecto de servicio	"Política de cuenta de servicio de conector"	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	storage.admin miembro: Cuenta de servicio de BlueXP como serviceAccount.user	N.A.	(Opcional) para la organización de datos en niveles y el backup y recuperación de BlueXP
Agente de servicio de API de Google	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	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	(Predeterminado) Editor	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.

Paso 5: Habilita las API de Google Cloud

Se deben habilitar varias API de Google Cloud antes de poder implementar Connector y Cloud Volumes ONTAP en Google Cloud.

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)
   - API del servicio de gestión de claves de cloud (KMS)

     (Solo es obligatorio si piensas utilizar el backup y la recuperación de datos de BlueXP con claves de cifrado gestionadas por el cliente (CMEK))

"Documentación de Google Cloud: Habilitar API"

Paso 6: Crear el conector

Crea un conector directamente desde la consola web de BlueXP o mediante gcloud.

Acerca de esta tarea

La creación de Connector implementa una instancia de máquina virtual en Google Cloud mediante una configuración predeterminada. Después de crear el conector, no debe cambiar a una instancia de VM más pequeña que tenga menos CPU o RAM. "Obtenga información sobre la configuración predeterminada para el conector".

BlueXP

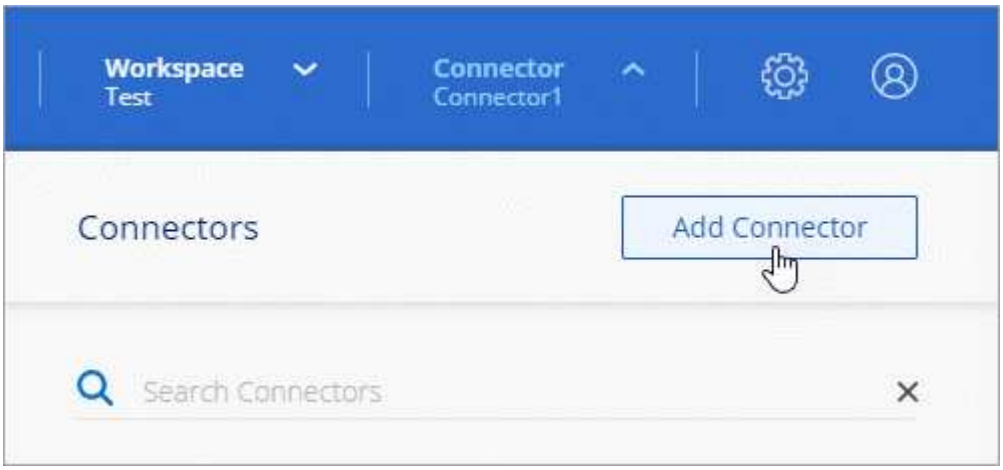
Antes de empezar

Debe tener lo siguiente:

- Los permisos necesarios de Google Cloud para crear el conector y una cuenta de servicio para el conector VM.
- Un VPC y una subred que cumplan los requisitos de red.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector.

Pasos

1. Seleccione la lista desplegable **Connector** y seleccione **Add Connector**.



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. Seleccione **Continuar** para prepararse para la implementación mediante la guía del producto. Cada paso de la guía del producto incluye la información que se incluye en esta página de la documentación.
   b. Selecciona **Saltar a la implementación** si ya lo preparaste 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.
   - **Política de firewall**: Elija si desea crear una nueva política de firewall o si desea seleccionar una política de firewall existente que permita las reglas de entrada y salida requeridas.

"Reglas de firewall en Google Cloud"

- **Revisión**: Revise sus selecciones para verificar que su configuración es correcta.

5. Seleccione **Agregar**.

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

Resultado

Una vez completado el proceso, el conector está disponible para su uso en BlueXP.

Si tienes buckets de Google Cloud Storage en la misma cuenta de Google Cloud en la que creaste el conector, verás que el entorno de trabajo de Google Cloud Storage aparece automáticamente en el lienzo de BlueXP. "Descubre cómo gestionar Google Cloud Storage desde BlueXP"

gcloud

Antes de empezar

Debe tener lo siguiente:

- Los permisos necesarios de Google Cloud para crear el conector y una cuenta de servicio para el conector VM.
- Un VPC y una subred que cumplan los requisitos de red.
- Comprensión de los requisitos de instancia de VM.
  - **CPU**: 4 núcleos o 4 vCPU
  - **RAM**: 14 GB
  - * Tipo de máquina *: Recomendamos n2-standard-4.

    El conector es compatible con Google Cloud en una instancia de VM con un SO que admite las características de VM blindadas.

Pasos

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 BlueXP que desea asociar al conector.

      "Obtenga más información sobre las cuentas de BlueXP".

   b. Escriba un nombre para el sistema.

Resultado

El conector ya está instalado y configurado con su cuenta BlueXP.

Abra un explorador web y vaya al "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Instale manualmente el conector en Google Cloud

Para instalar manualmente el conector en su propio host Linux, debe revisar los requisitos del host, configurar la red, preparar los permisos de Google Cloud, habilitar las API de Google Cloud, instalar el conector y, a continuación, proporcionar los permisos que preparó.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Revise 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.

Host dedicado

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

Sistemas operativos compatibles

- Sistema operativo Ubuntu 22,04 LTS
- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7,6, 7,7, 7,8 y 7,9

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

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

Hipervisor

Se requiere un hipervisor con configuración básica o alojado certificado para ejecutar Ubuntu, CentOS o Red Hat Enterprise Linux.

"Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"

CPU

4 núcleos o 4 vCPU

RAM

14 GB

Tipo de máquina de Google Cloud

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"

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 en el host antes de instalar Connector.

- La versión mínima admitida es 19,3.1.
- La versión máxima admitida es 25,0.5.

  "Ver las instrucciones de instalación"

Paso 2: Configurar redes

Configure su red para que Connector pueda gestionar recursos y procesos en su entorno de cloud híbrido. Por ejemplo, debe asegurarse de que las conexiones estén disponibles para las redes de destino y de que el

acceso a Internet de salida esté disponible.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados durante la instalación manual

Al instalar manualmente el conector en su propio host Linux, el instalador del conector requiere acceso 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://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  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.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://www.googleapis.com/compute/v1/ https://compute.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 https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	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 de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Paso 3: Configurar permisos para el conector

Se necesita una cuenta de servicio de Google Cloud para proporcionar al Connector los permisos que BlueXP necesita para gestionar recursos en Google Cloud. Cuando cree el Connector, deberá asociar esta cuenta de servicio con la VM de Connector.

Pasos

1. Cree un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya el contenido de "Permisos de cuenta de servicio para el conector".

   b. Desde Google Cloud, active Cloud Shell.

   c. Cargue el archivo YAML que incluya los permisos necesarios.

   d. Cree un rol personalizado mediante `gcloud iam roles create` comando.

      En el ejemplo siguiente se crea una función denominada "conector" en el nivel de proyecto:

      ```
      gcloud iam roles create connector --project=myproject --file=connector.yaml
      ```

   "Documentos de Google Cloud: Creación y gestión de roles personalizados"

2. Cree una cuenta de servicio en Google Cloud y asígnele el rol a la cuenta de servicio:

   a. En el servicio IAM y Admin, selecciona **Cuentas de servicio > Crear cuenta de servicio**.

   b. Ingrese los detalles de la cuenta de servicio y seleccione **Crear y continuar**.

   c. Seleccione la función que acaba de crear.

   d. Finalice los pasos restantes para crear la función.

      "Documentos de Google Cloud: Crear una cuenta de servicio"

3. 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.

   a. En el servicio IAM & Admin, seleccione el proyecto de Google Cloud en el que desea crear sistemas Cloud Volumes ONTAP.

   b. 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.
      - Seleccione **Guardar**.

   Para obtener información detallada, consulte "Documentación de Google Cloud"

Resultado

Se ha configurado la cuenta de servicio del conector VM.

Paso 4: Configurar permisos de VPC compartidos

Si utiliza un VPC compartido para implementar recursos en un proyecto de servicio, tendrá que preparar los permisos.

Esta tabla es de referencia y el entorno debe reflejar la tabla de permisos cuando se haya completado la configuración de IAM.

Ver permisos de VPC compartidos

Identidad	Creador	Alojadas en	Permisos de proyecto de servicio	Permisos del proyecto host	Específico
Cuenta de Google para desplegar el conector	Personalizado	Proyecto de servicio	"Política de despliegue de conectores"	compute.networkUser	Despliegue del conector en el proyecto de servicio
Cuenta de servicio del conector	Personalizado	Proyecto de servicio	"Política de cuenta de servicio de conector"	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	storage.admin miembro: Cuenta de servicio de BlueXP como serviceAccount.user	N.A.	(Opcional) para la organización de datos en niveles y el backup y recuperación de BlueXP
Agente de servicio de API de Google	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	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	(Predeterminado) Editor	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.

Paso 5: Habilita las API de Google Cloud

Se deben habilitar varias API de Google Cloud antes de poder implementar sistemas de Cloud Volumes ONTAP en Google Cloud.

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)
   - API del servicio de gestión de claves de cloud (KMS)

     (Solo es obligatorio si piensas utilizar el backup y la recuperación de datos de BlueXP con claves de cifrado gestionadas por el cliente (CMEK))

"Documentación de Google Cloud: Habilitar API"

Paso 6: Instale el conector

Una vez completados los requisitos previos, puede instalar manualmente el software en su propio host Linux.

Antes de empezar

Debe tener lo siguiente:

- 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.

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

  Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

- Un certificado firmado por CA, si el servidor proxy utiliza HTTPS o si el proxy es un proxy de interceptación.

Acerca de esta tarea

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 "en línea" del conector que se utiliza en su red o en la nube. Hay disponible un instalador "sin conexión" independiente para el conector, pero sólo es compatible con implementaciones en modo privado.

4. Asigne permisos para ejecutar el script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Ejecute el script de instalación.

```
 ./BlueXP-Connector-Cloud-<version> --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:

```
 ./BlueXP-Connector-Cloud-v3.9.38 --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://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port

- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Tenga en cuenta lo siguiente:

  - El usuario puede ser un usuario local o un usuario de dominio.
  - Para un usuario de dominio, debe utilizar el código ASCII para \ como se muestra anteriormente.
  - BlueXP no admite contraseñas que incluyan el carácter @.

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

6. Espere a que finalice la instalación.

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

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

   https://ipaddress

8. Después de iniciar sesión, configure el conector:
   a. Especifique la cuenta BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y está configurado con su cuenta BlueXP.

Si tienes buckets de Google Cloud Storage en la misma cuenta de Google Cloud en la que creaste el conector, verás que el entorno de trabajo de Google Cloud Storage aparece automáticamente en el lienzo de BlueXP. "Descubre cómo gestionar Google Cloud Storage desde BlueXP"

Paso 7: Proporcionar permisos a BlueXP

Tienes que proporcionar a BlueXP los permisos de Google Cloud que hayas configurado anteriormente. Al proporcionar los permisos, BlueXP podrá gestionar tus datos y la infraestructura de almacenamiento en Google Cloud.

Pasos

1. Vaya al portal de Google Cloud y asigne la cuenta de servicio a la instancia de Connector VM.

   "Documentación de Google Cloud: Cambiar la cuenta de servicio y los ámbitos de acceso para una

instancia"

2. Si quieres gestionar recursos en otros proyectos de Google Cloud, otorga acceso agregando la cuenta de servicio con el rol de BlueXP a ese proyecto. Deberá repetir este paso con cada proyecto.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Google Cloud en su nombre.

Instalar y configurar un conector en las instalaciones

Instale un conector en las instalaciones y, a continuación, inicie sesión y configúrelo para que funcione con su cuenta de BlueXP.

Antes de empezar

Usted debe revisar "Limitaciones del conector".

Paso 1: Revise 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. Asegúrese de que el host cumple estos requisitos antes de instalar el conector.

Host dedicado

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

Sistemas operativos compatibles

- Sistema operativo Ubuntu 22,04 LTS
- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7,6, 7,7, 7,8 y 7,9

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

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

Hipervisor

Se requiere un hipervisor con configuración básica o alojado certificado para ejecutar Ubuntu, CentOS o Red Hat Enterprise Linux.

"Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"

CPU

4 núcleos o 4 vCPU

RAM

14 GB

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 en el host antes de instalar Connector.

- La versión mínima admitida es 19,3.1.
- La versión máxima admitida es 25,0.5.

"Ver las instrucciones de instalación"

Paso 2: Configurar redes

Configure su red para que Connector pueda gestionar recursos y procesos en su entorno de cloud híbrido. Por ejemplo, debe asegurarse de que las conexiones estén disponibles para las redes de destino y de que el acceso a Internet de salida esté disponible.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados durante la instalación manual

Al instalar manualmente el conector en su propio host Linux, el instalador del conector requiere acceso 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://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  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.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://www.googleapis.com/compute/v1/ https://compute.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 https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.

Puntos finales	Específico
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	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 de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Paso 3: Configure los permisos de la nube

Si quieres usar los servicios de BlueXP en AWS o Azure con un conector on-premises, necesitas configurar permisos en tu proveedor de nube para que puedas añadir las credenciales al conector después de instalarlo.

¿Por qué no Google Cloud? Cuando Connector está instalado en las instalaciones, no puede gestionar sus recursos en Google Cloud. El conector debe estar instalado en Google Cloud para administrar los recursos que residen allí.

AWS

Cuando el conector está instalado en las instalaciones, debe proporcionar permisos de BlueXP con AWS agregando claves de acceso para un usuario de IAM que tenga los permisos necesarios.

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

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:

   a. Selecciona **Políticas > Crear política**.

   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".

   c. Finalice los pasos restantes para crear la directiva.

      Dependiendo de los servicios de BlueXP que tenga previsto utilizar, puede que necesite crear una segunda política.

   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. "Obtenga más información sobre las políticas de IAM para el conector".

3. Adjunte las políticas a un usuario de IAM.
   - "Documentación de AWS: Crear roles de IAM"
   - "Documentación de AWS: Adición y eliminación de políticas de IAM"
4. Asegúrese de que el usuario tiene una clave de acceso que puede agregar a BlueXP después de instalar el conector.

Resultado

Ahora debe tener claves de acceso para un usuario de IAM que tenga los permisos necesarios. Después de instalar el conector, deberá asociar estas credenciales con el conector de BlueXP.

Azure

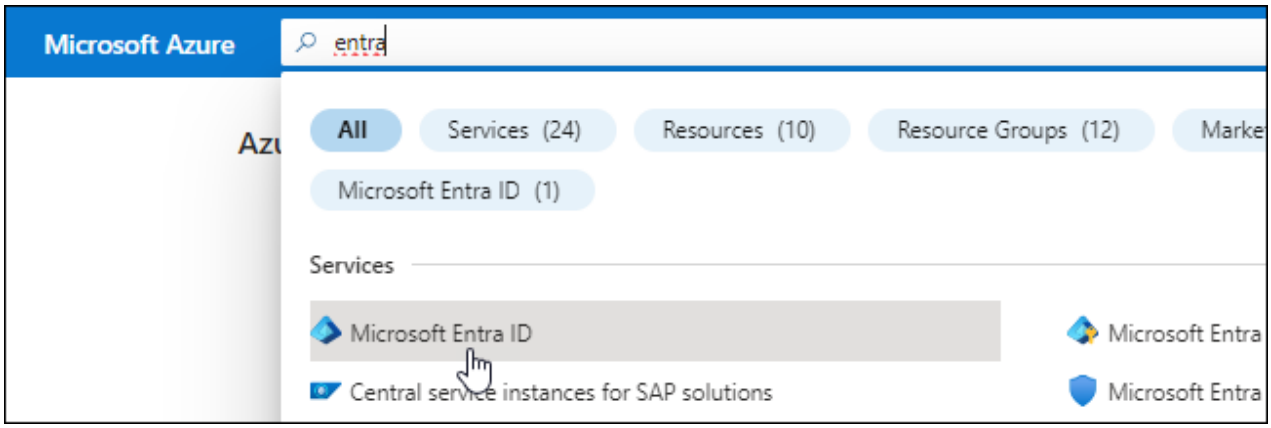
Cuando Connector se instala en las instalaciones, tendrás que proporcionar permisos de Azure a BlueXP configurando un principal de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que necesita BlueXP.

Cree una aplicación Microsoft Entra para el control de acceso basado en roles

1. Asegúrese de tener permisos en Azure para crear una aplicación de Active Directory y para asignar la aplicación a un rol.

   Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios"

2. Desde el portal de Azure, abra el servicio **Microsoft Entra ID**.



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. 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.
6. Seleccione **Registrar**.

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

   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.

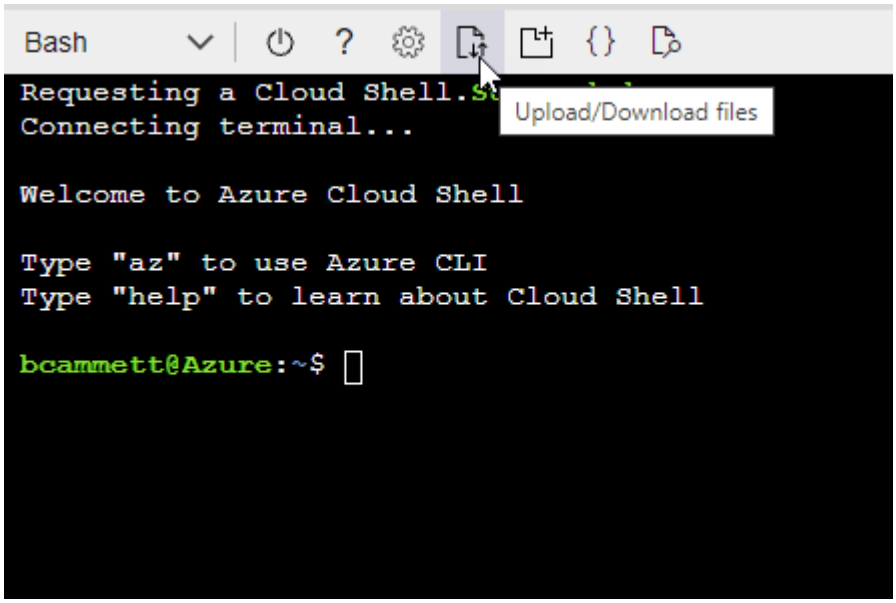
      ejemplo

      ```
      "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:

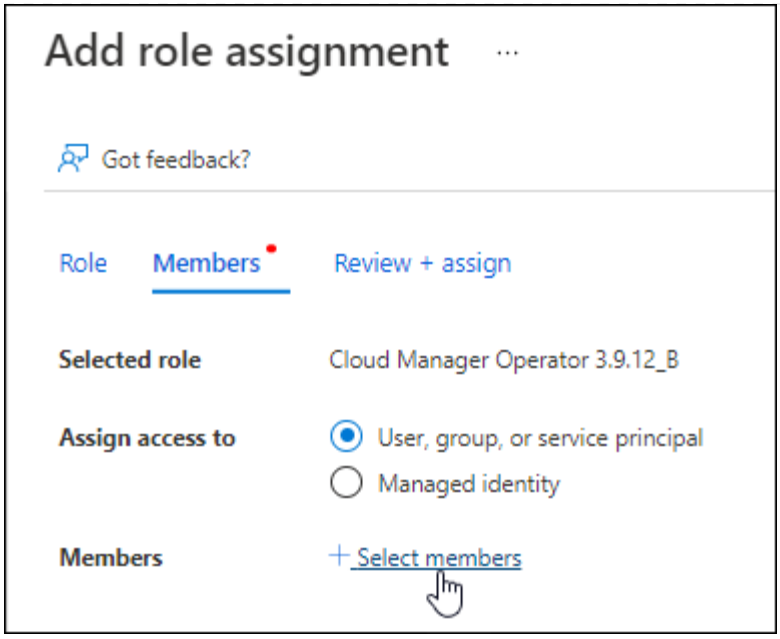
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

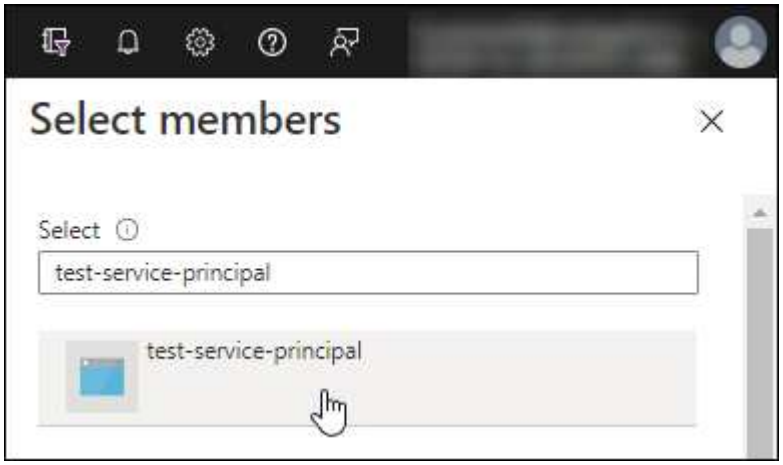
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**, realice los siguientes pasos:

      - Mantener seleccionado **Usuario, grupo o principal de servicio**.
      - Seleccione **Seleccionar miembros**.



- Busque el nombre de la aplicación.

  Veamos un ejemplo:



- Seleccione la aplicación y seleccione **Seleccionar**.
- Seleccione **Siguiente**.

f. Seleccione **revisar + asignar**.

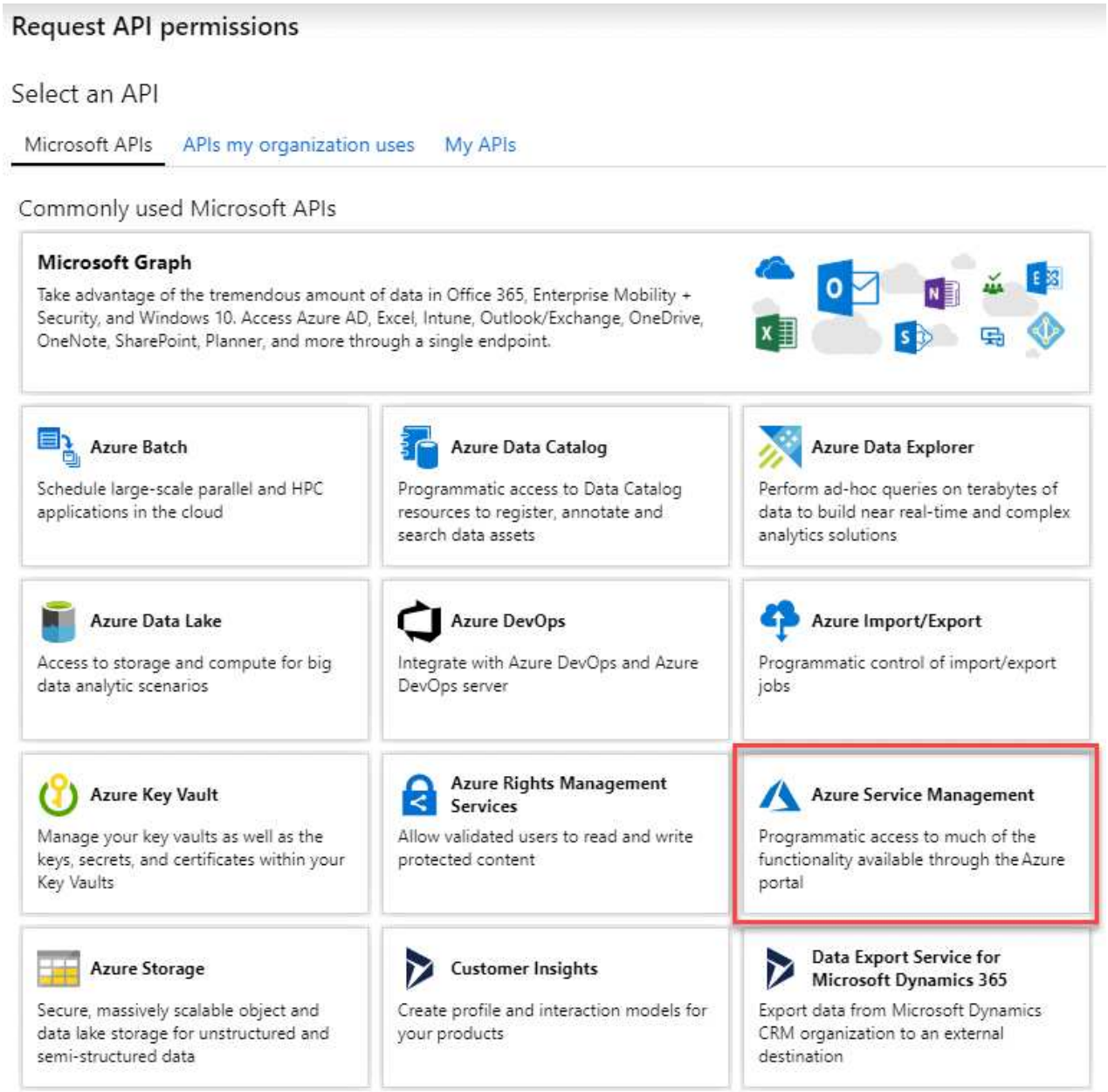
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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.

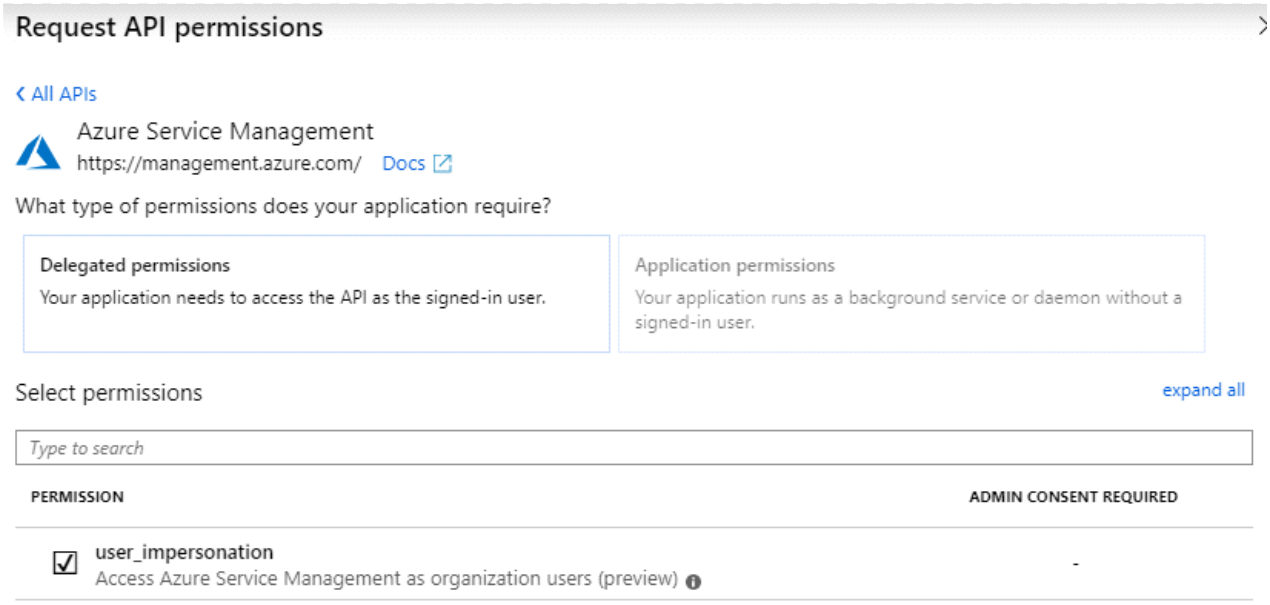
Añada permisos de API de administración de servicios de Windows Azure

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Seleccione **permisos de API > Agregar un permiso**.

3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.

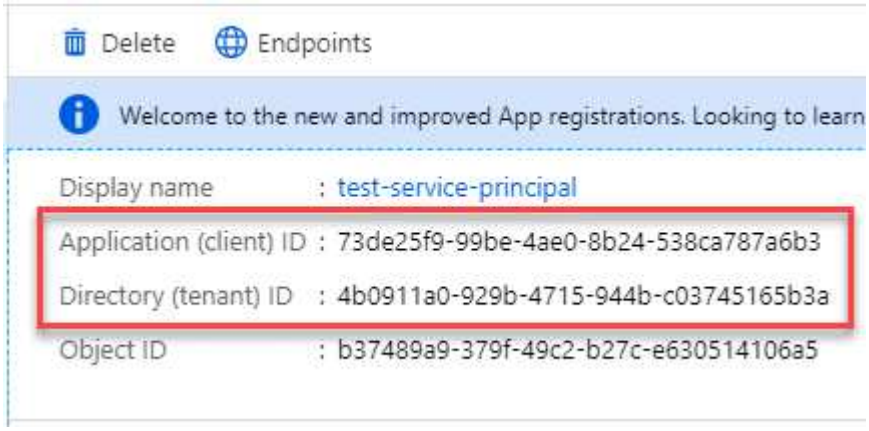


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



Obtenga el ID de aplicación y el ID de directorio de la aplicación

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Cree un secreto de cliente

1. Abra el servicio **Microsoft Entra ID**.
2. Seleccione **App registres** y seleccione su aplicación.
3. Seleccione **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copie el valor del secreto de cliente.

Ahora tienes un secreto de cliente que BlueXP puede usarlo para autenticar con Microsoft Entra ID.

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. Después de instalar el conector, deberá asociar estas credenciales con el conector de BlueXP.

Paso 4: Instale el conector

Descargue e instale el software Connector en un host Linux existente de forma local.

Antes de empezar

Debe tener lo siguiente:

- 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.

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

  Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

- Un certificado firmado por CA, si el servidor proxy utiliza HTTPS o si el proxy es un proxy de interceptación.

Acerca de esta tarea

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 "en línea" del conector que se utiliza en su red o en la nube. Hay disponible un instalador "sin conexión" independiente para el conector, pero sólo es compatible con implementaciones en modo privado.

4. Asigne permisos para ejecutar el script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

5. Ejecute el script de instalación.

```
 ./BlueXP-Connector-Cloud-<version> --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:

```
 ./BlueXP-Connector-Cloud-v3.9.38 --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://user-name:password@address:port
   - http://domain-name%92user-name:password@address:port
   - https://address:port
   - https://user-name:password@address:port
   - https://domain-name%92user-name:password@address:port

     Tenga en cuenta lo siguiente:

     - El usuario puede ser un usuario local o un usuario de dominio.
     - Para un usuario de dominio, debe utilizar el código ASCII para \ como se muestra anteriormente.
     - BlueXP no admite contraseñas que incluyan el carácter @.

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

es un proxy de interceptación.

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.

Paso 5: Configure el conector

Inicia sesión o inicia sesión y, a continuación, configura el conector para que funcione con tu cuenta de BlueXP.

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. Después de iniciar sesión, configure BlueXP:
   a. Especifique la cuenta BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. (Además, el modo restringido no es compatible cuando el conector está instalado en las instalaciones.)

   d. Selecciona **Comenzar**.

Resultado

BlueXP está ahora configurado con el conector que acaba de instalar.

Paso 6: Proporcionar permisos a BlueXP

Después de instalar y configurar Connector, añada sus credenciales del cloud para que BlueXP tenga los permisos necesarios para realizar acciones en AWS o Azure.

AWS

Antes de empezar

Si acaba de crear estas credenciales en AWS, puede tardar varios minutos en estar disponible para su uso. Espere unos minutos antes de agregar las credenciales a BlueXP.

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Servicios Web de Amazon > conector**.
   b. **Definir credenciales**: Introduzca una clave de acceso y una clave secreta de AWS.
   c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.
   d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

Ahora puede ir al "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Azure

Antes de empezar

Si acaba de crear estas credenciales en Azure, es posible que tardé unos minutos en poder utilizarlas. Espere unos minutos antes de agregar las credenciales a BlueXP.

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.
   b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:
      - ID de aplicación (cliente)
      - ID de directorio (inquilino)
      - Secreto de cliente

c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre. Ahora puede ir al "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Suscribirse a BlueXP (modo estándar)

Suscríbase a BlueXP en el mercado de su proveedor de la nube para pagar los servicios de BlueXP a una tarifa por hora (PAYGO) o a través de un contrato anual. Si adquirió una licencia de NetApp (BYOL), también deberá suscribirse a la oferta de mercado. Su licencia siempre se cobra primero, pero se le cobrará la tarifa por hora si excede la capacidad de su licencia o si el plazo de la licencia expira.

Una suscripción al mercado permite cargar los siguientes servicios de BlueXP:

- Backup y recuperación
- Clasificación
- Cloud Volumes ONTAP
- Organización en niveles

Antes de empezar

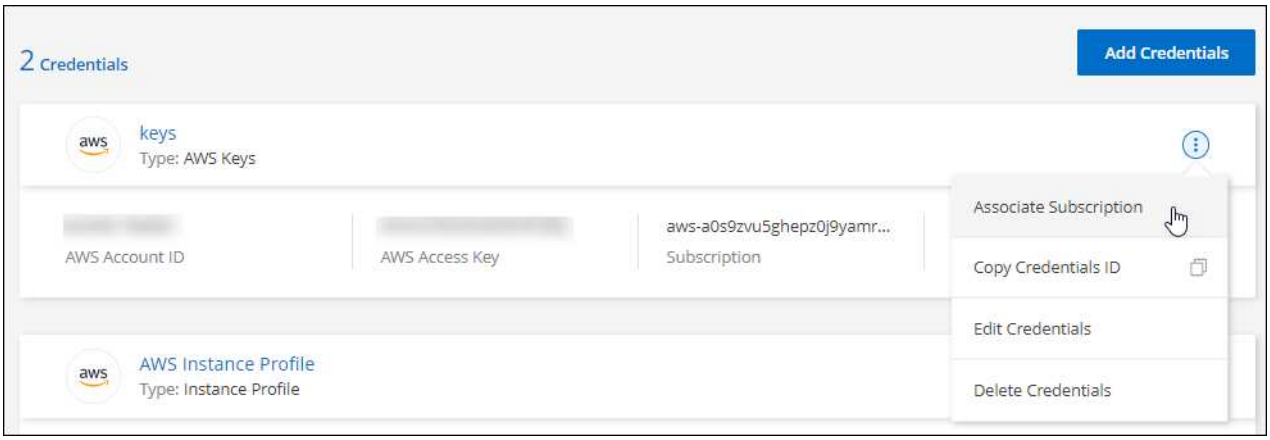
La suscripción a BlueXP implica asociar una suscripción al mercado con las credenciales de la nube asociadas con un conector. Si ha seguido el flujo de trabajo para empezar con el modo estándar, ya debe tener un conector. Para obtener más información, consulte la "Inicio rápido para BlueXP en modo estándar".

AWS

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y seleccione **asociado**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos del AWS Marketplace:

   a. Seleccione **Ver opciones de compra**.

   b. Seleccione **Suscribirse**.

   c. Seleccione **Configurar su cuenta**.

      Se le redirigirá al sitio web de BlueXP.

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

      - Seleccione las cuentas de BlueXP con 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.

      - Seleccione **Guardar**.

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

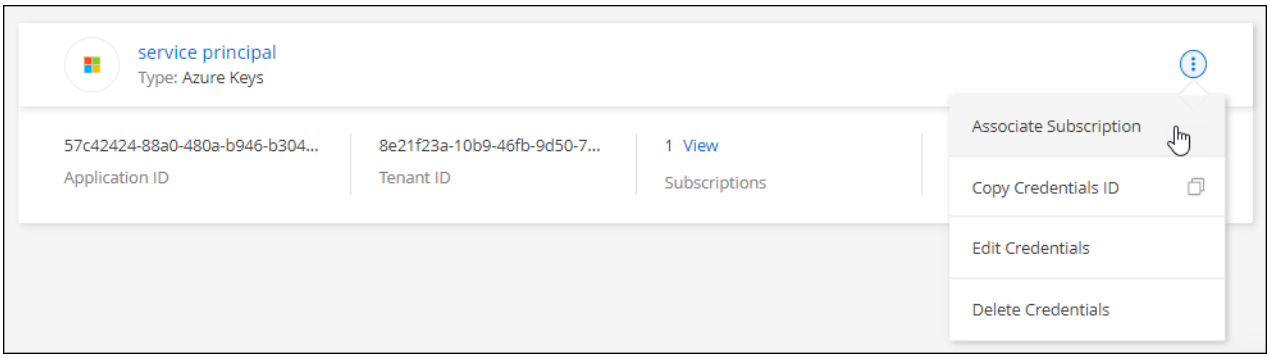
Suscríbete a BlueXP desde AWS Marketplace

Azure

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y seleccione **asociado**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos de Azure Marketplace:

   a. Si se le solicita, inicie sesión en su cuenta de Azure.

   b. Seleccione **Suscribirse**.

   c. Rellene el formulario y seleccione **Suscribirse**.

   d. Una vez completado el proceso de suscripción, seleccione **Configurar cuenta ahora**.

      Se le redirigirá al sitio web de BlueXP.

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

      - Seleccione las cuentas de BlueXP con 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.

      - Seleccione **Guardar**.

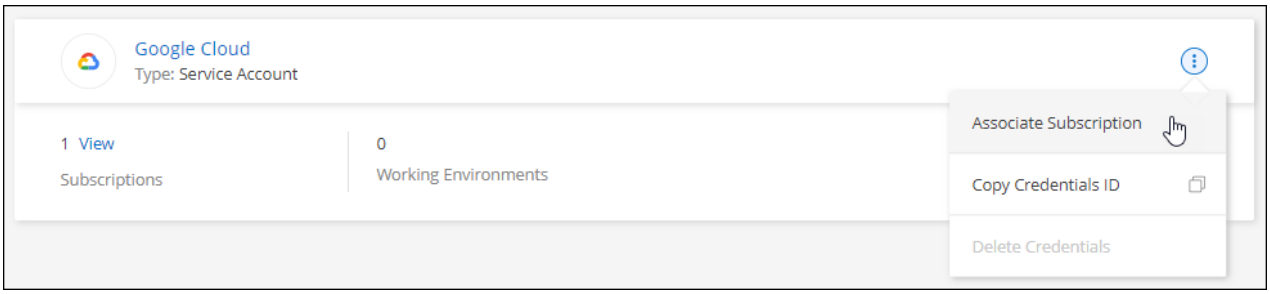
        En el siguiente vídeo se muestran los pasos para suscribirse desde Azure Marketplace:

   Suscríbete a BlueXP desde Azure Marketplace

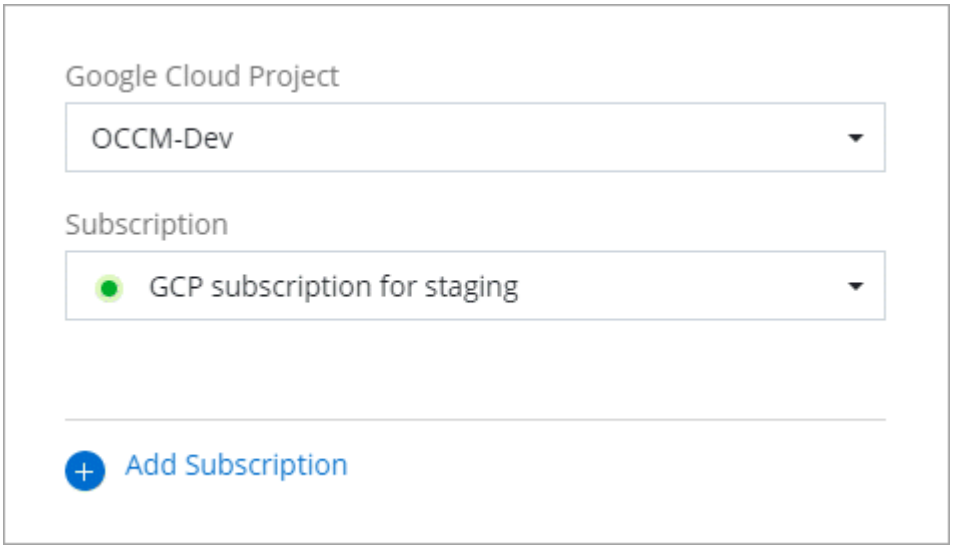
Google Cloud

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.



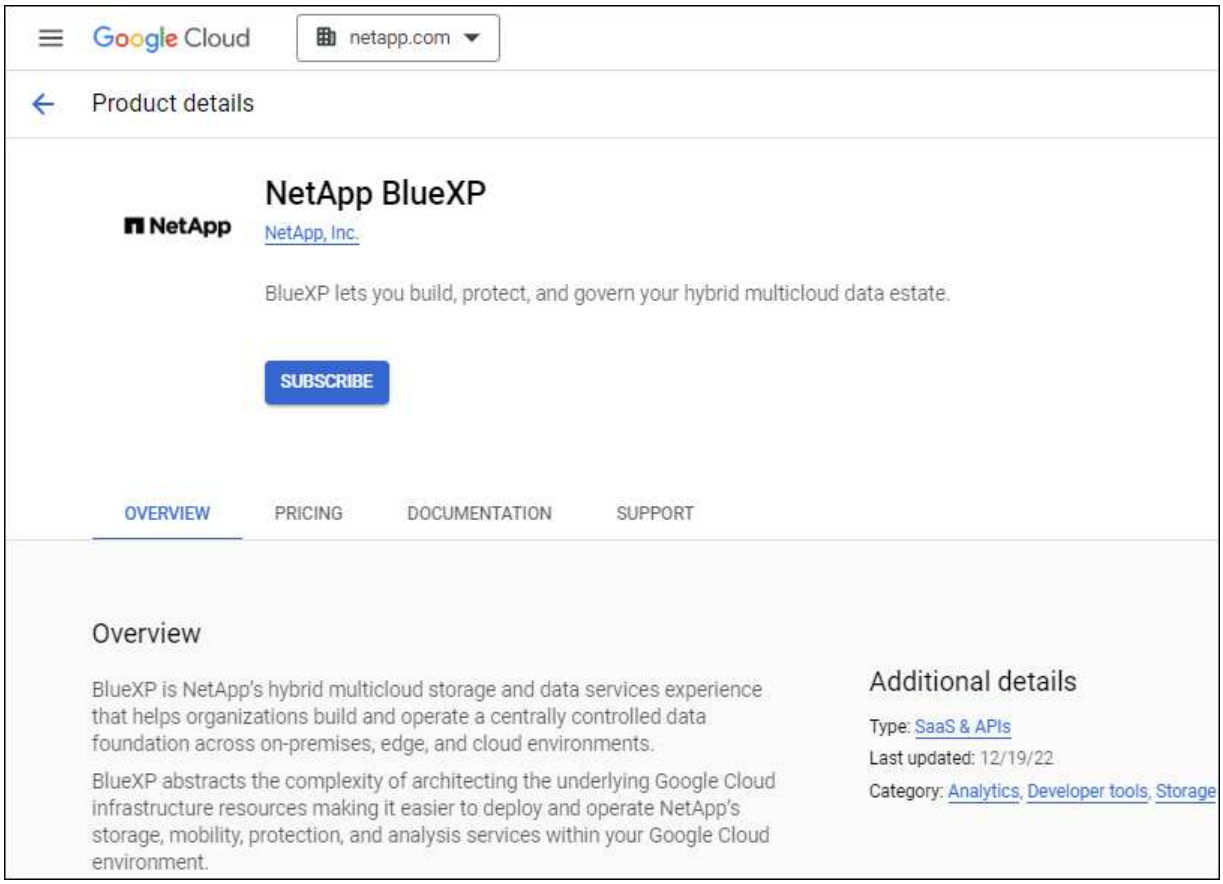
3. Para asociar las credenciales a una suscripción existente, seleccione un proyecto de Google Cloud y una suscripción en la lista desplegable y, a continuación, seleccione **asociado**.



4. Si aún no tiene una suscripción, seleccione **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.



b. Seleccione **Suscribirse**.

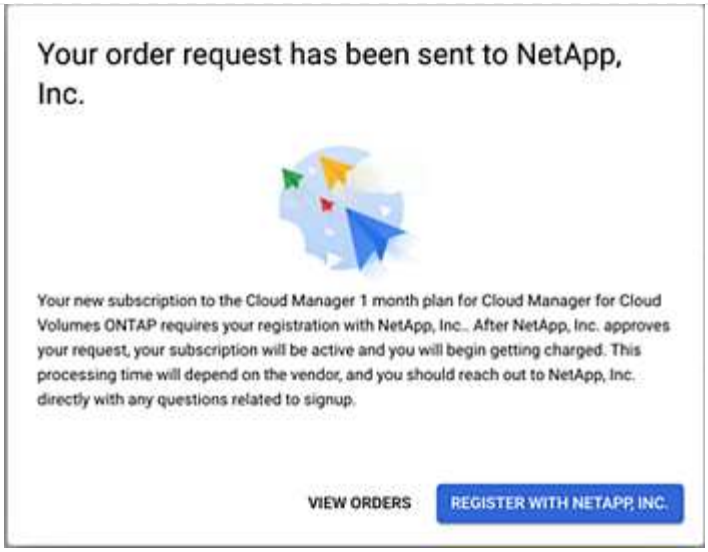
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.

d. Seleccione **Suscribirse**.

   Este paso envía la solicitud de transferencia a NetApp.

e. En el cuadro de diálogo emergente, seleccione **Registro con NetApp, Inc.**

   Este paso debe completarse para vincular la suscripción a Google Cloud a su cuenta de BlueXP. 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 BlueXP con 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.

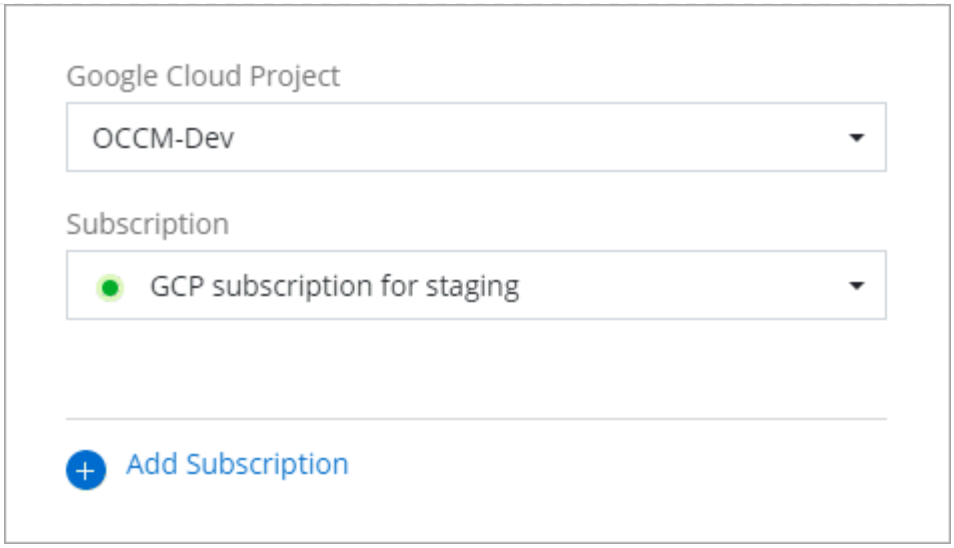
Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

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

Suscríbete a BlueXP desde Google Cloud Marketplace

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



Enlaces relacionados

- "Gestione las licencias basadas en la capacidad de su propia licencia para Cloud Volumes ONTAP"
- "Gestiona las licencias BYOL para los servicios de datos de BlueXP"
- "Gestione las credenciales y suscripciones de AWS para BlueXP"
- "Gestione credenciales y suscripciones de Azure para BlueXP"
- "Administrar las credenciales y suscripciones de Google Cloud para BlueXP"

Qué puede hacer después (modo estándar)

Ahora que ha iniciado sesión y configurado BlueXP en modo estándar, los usuarios pueden crear y descubrir entornos de trabajo y utilizar servicios de datos BlueXP.

> Si instaló un Connector en AWS, Microsoft Azure o Google Cloud, BlueXP detecta automáticamente información sobre los buckets de Amazon S3, el almacenamiento de Azure Blob o los buckets de Google Cloud Storage en la ubicación donde se instaló Connector. Se agrega automáticamente un entorno de trabajo al lienzo de BlueXP.

Para obtener ayuda, vaya al "página principal de la documentación de BlueXP" Para ver los documentos de todos los servicios de BlueXP.

Enlace relacionado

"Modos de implementación de BlueXP"

Comience con el modo restringido

Flujo de trabajo inicial (modo restringido)

Empieza a usar BlueXP en modo restringido preparando tu entorno, poniendo en marcha Connector y suscribiéndote a BlueXP.

El modo restringido suele ser utilizado por los gobiernos estatales y locales y las empresas reguladas,

incluidas las implementaciones en las regiones AWS GovCloud y Azure Government. Antes de empezar, debería comprender "Cuentas BlueXP", "Conectores", y. "modos de despliegue".

1 **"Prepárese para la puesta en marcha"**

1. Prepare un host de Linux dedicado que cumpla los requisitos de CPU, RAM, espacio en disco, Docker Engine y mucho más.
2. Configure redes que proporcionen acceso a las redes de destino, acceso saliente a Internet para instalaciones manuales e Internet saliente para el acceso diario.
3. Configure los permisos en el proveedor de cloud para que pueda asociar dichos permisos a la instancia de Connector después de implementarla.

2 **"Despliegue el conector"**

1. Instale el conector desde el mercado de su proveedor de cloud o instalando manualmente el software en su propio host Linux.
2. Configure BlueXP abriendo un navegador Web e introduciendo la dirección IP del host Linux.
3. Proporcione a BlueXP los permisos que configuró anteriormente.

3 **"Suscríbase a BlueXP"**

Suscríbase a BlueXP en el mercado de su proveedor de la nube para pagar los servicios de BlueXP a una tarifa por hora (PAYGO) o a través de un contrato anual.

Preparación para la puesta en marcha en modo restringido

Prepara tu entorno antes de poner en marcha BlueXP en modo restringido. Por ejemplo, debe revisar los requisitos del host, preparar redes, configurar permisos y mucho más.

Paso 1: Entender cómo funciona el modo restringido

Antes de empezar, debe tener una comprensión de cómo funciona BlueXP en modo restringido.

Por ejemplo, debe entender que necesita utilizar la interfaz basada en explorador que está disponible localmente desde el conector BlueXP que necesita instalar. No puede acceder a BlueXP desde la consola basada en Web que se proporciona a través de la capa SaaS.

Además, no todos los servicios de BlueXP están disponibles.

"Descubra cómo funciona el modo restringido".

Paso 2: Revise las opciones de instalación

En el modo restringido, sólo puede instalar el conector en la nube. Están disponibles las siguientes opciones de instalación:

- Desde el AWS Marketplace
- Desde Azure Marketplace

- Instalación manual del conector en su propio host Linux que se ejecuta en AWS, Azure o Google Cloud

Paso 3: Revise 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.

Al poner en marcha el conector desde AWS o Azure Marketplace, la imagen incluye el sistema operativo y los componentes de software necesarios. Simplemente tiene que elegir un tipo de instancia que cumpla con los requisitos de CPU y RAM.

Host dedicado

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

Sistemas operativos compatibles

- Sistema operativo Ubuntu 22,04 LTS
- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7,6, 7,7, 7,8 y 7,9

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

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

Hipervisor

Se requiere un hipervisor con configuración básica o alojado certificado para ejecutar Ubuntu, CentOS o Red Hat Enterprise Linux.

"Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"

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 de Google Cloud

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"

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 en el host antes de instalar Connector.

- La versión mínima admitida es 19,3.1.
- La versión máxima admitida es 25,0.5.

"Ver las instrucciones de instalación"

Paso 4: Preparar el networking

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.

Conexiones a redes de destino

El conector debe tener una conexión de red a la ubicación en la que desea gestionar el almacenamiento. Por ejemplo, el VPC o vnet donde planea poner en marcha Cloud Volumes ONTAP, o el centro de datos donde residen los clústeres de ONTAP en las instalaciones.

Preparar la red para el acceso de los usuarios a la consola BlueXP

En modo restringido, se puede acceder a la interfaz de usuario de BlueXP desde el conector. Al utilizar la interfaz de usuario de BlueXP, se pone en contacto con unos pocos extremos para completar las tareas de gestión de datos. Estos extremos se ponen en contacto desde el equipo de un usuario al completar acciones específicas desde la consola de BlueXP.

Puntos finales	Específico
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.

Puntos finales contactados durante la instalación manual

Al instalar manualmente el conector en su propio host Linux, el instalador del conector requiere acceso 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://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Este punto final no es necesario en las regiones gubernamentales de Azure.

- https://occmclientinfragov.azurecr.us

  Este extremo solo se requiere en las regiones gubernamentales de Azure.

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.

Acceso a Internet saliente para operaciones diarias

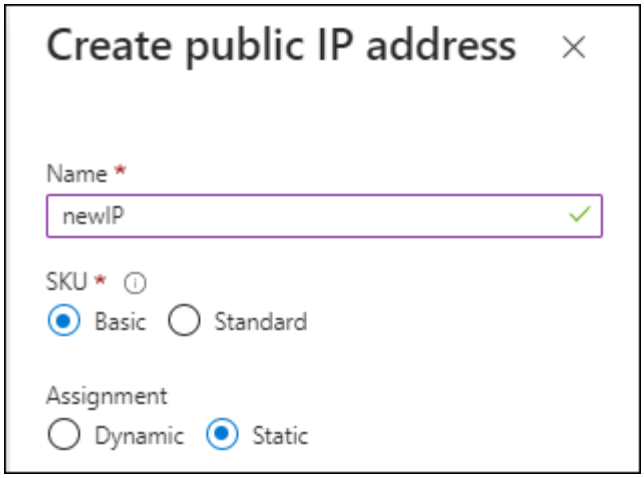
La ubicación de red en la que implemente el conector debe tener una conexión a Internet saliente. El conector requiere acceso saliente a Internet para ponerse en contacto con los siguientes extremos con el fin de gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Para gestionar recursos en regiones gubernamentales de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.

Puntos finales	Específico
https://www.googleapis.com/compute/v1/ https://compute.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 https://mysupport.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 https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Este punto final no es necesario en las regiones gubernamentales de Azure. https://occmclientinfragov.azurecr.us Este extremo solo se requiere en las regiones gubernamentales de Azure.	Para actualizar el conector y sus componentes de Docker.

La dirección IP pública en Azure

Si desea utilizar una dirección IP pública con Connector VM en Azure, la dirección IP debe utilizar una SKU básica para garantizar que BlueXP utilice esta dirección IP pública.



Si en su lugar utiliza una dirección IP de SKU estándar, BlueXP utiliza la dirección *private* IP del conector, en lugar de la dirección IP pública. Si el equipo que está utilizando para acceder a la consola BlueXP no tiene acceso a esa dirección IP privada, las acciones de la consola BlueXP fallarán.

"Documentación para Azure: SKU de IP pública"

Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- 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.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en 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.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más

información sobre la clasificación de BlueXP"

Si está planeando crear el conector desde el mercado de su proveedor de nube, deberá implementar este requisito de red después de crear el conector.

Paso: 5 Prepare los permisos en la nube

BlueXP requiere permisos de su proveedor de cloud para poner en marcha Cloud Volumes ONTAP en una red virtual y para utilizar servicios de datos BlueXP. Debe configurar permisos en su proveedor de cloud y, a continuación, asociar dichos permisos con el conector.

Para ver los pasos requeridos, seleccione la opción de autenticación que desee usar para su proveedor de cloud.

Rol IAM de AWS

Utilice un rol de IAM para proporcionar al conector permisos.

Si está creando el conector desde AWS Marketplace, se le pedirá que seleccione ese rol IAM al iniciar la instancia de EC2.

Si está instalando manualmente el conector en su propio host Linux, tendrá que asociar el rol a la instancia de EC2.

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:
   a. Selecciona **Políticas > Crear política**.
   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".
   c. Finalice los pasos restantes para crear la directiva.
3. Cree un rol IAM:
   a. Selecciona **Roles > Crear rol**.
   b. Seleccione **Servicio AWS > EC2**.
   c. Agregue permisos asociando la directiva que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

Resultado

Ahora tiene un rol de IAM para la instancia de Connector EC2.

Clave de acceso de AWS

Configurar permisos y una clave de acceso para un usuario de IAM. Deberá proporcionar a BlueXP la clave de acceso de AWS después de instalar el conector y configurar BlueXP.

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:

   a. Selecciona **Políticas > Crear política**.
   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".
   c. Finalice los pasos restantes para crear la directiva.

      Dependiendo de los servicios de BlueXP que tenga previsto utilizar, puede que necesite crear una segunda política.

   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. "Obtenga más información sobre las políticas de IAM para el conector".

3. Adjunte las políticas a un usuario de IAM.
   - "Documentación de AWS: Crear roles de IAM"
   - "Documentación de AWS: Adición y eliminación de políticas de IAM"

4. Asegúrese de que el usuario tiene una clave de acceso que puede agregar a BlueXP después de instalar el conector.

Resultado

La cuenta ahora tiene los permisos necesarios.

Rol de Azure

Cree un rol personalizado de Azure con los permisos necesarios. Asignará este rol al conector VM.

Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

Pasos

1. Si tiene pensado instalar manualmente el software en su propio host, habilite una identidad gestionada asignada por el sistema en la máquina virtual para poder ofrecer los permisos de Azure necesarios a través de un rol personalizado.

   "Documentación de Microsoft Azure: Configure las identidades gestionadas para los recursos de Azure en una máquina virtual mediante el portal de Azure"

2. Copie el contenido de "Permisos de función personalizada para el conector" Y guárdelos en un archivo JSON.
3. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

   Debes añadir el ID de cada suscripción de Azure que quieras utilizar con BlueXP.

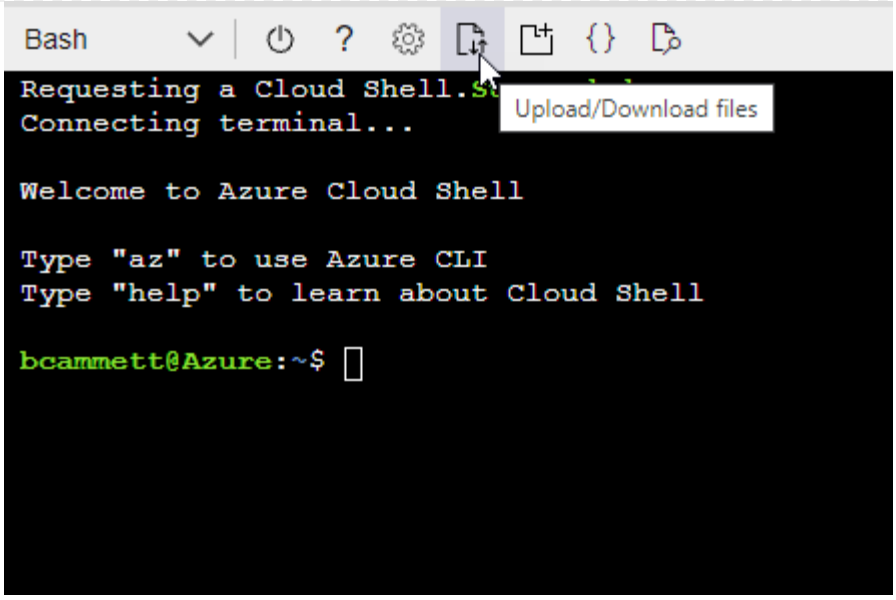
   ejemplo

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

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

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

Resultado

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

Servicio principal de Azure

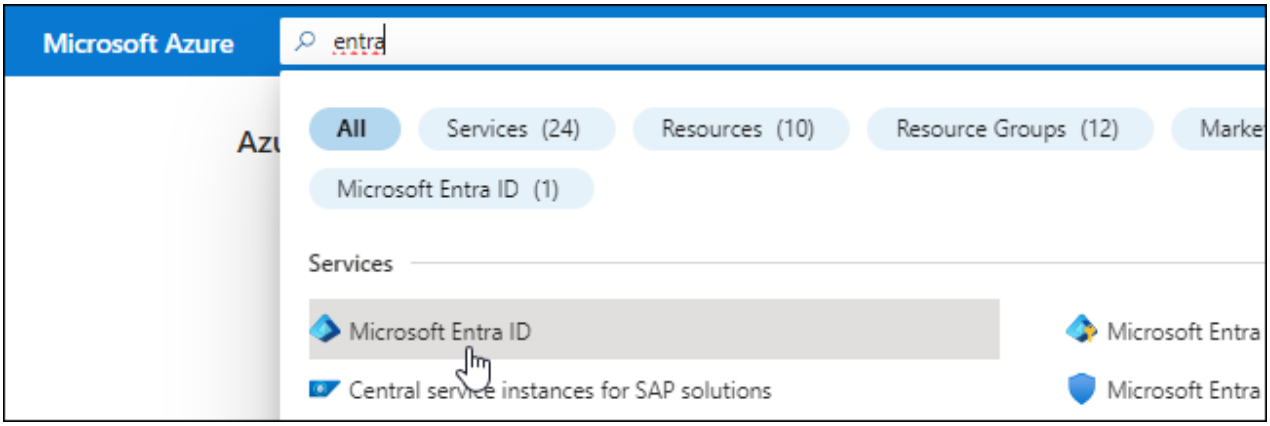
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita. Necesitará proporcionar estas credenciales a BlueXP después de instalar el conector y configurar BlueXP.

Cree una aplicación Microsoft Entra para el control de acceso basado en roles

1. Asegúrese de tener permisos en Azure para crear una aplicación de Active Directory y para asignar la aplicación a un rol.

   Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios"

2. Desde el portal de Azure, abra el servicio **Microsoft Entra ID**.



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. 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.
6. Seleccione **Registrar**.

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

   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.

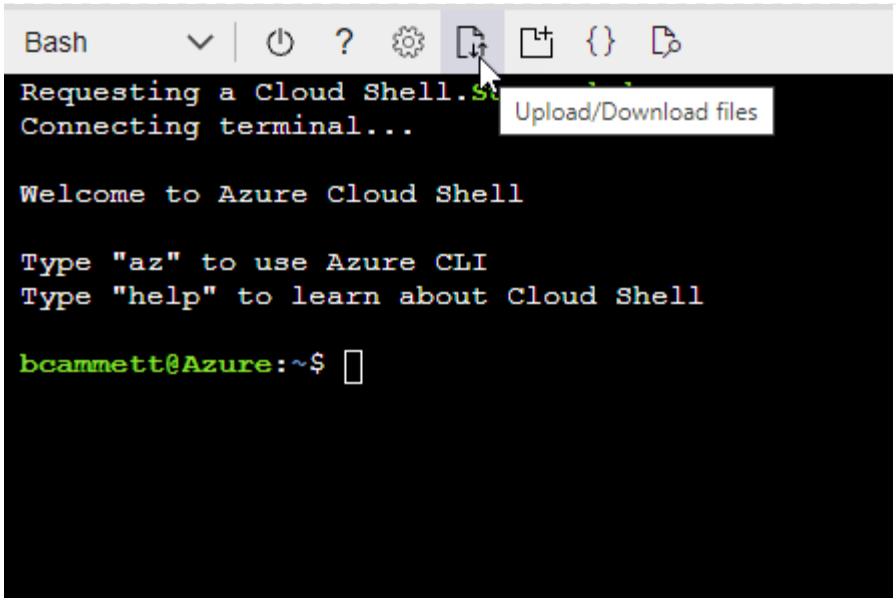
      ejemplo

      ```
      "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:

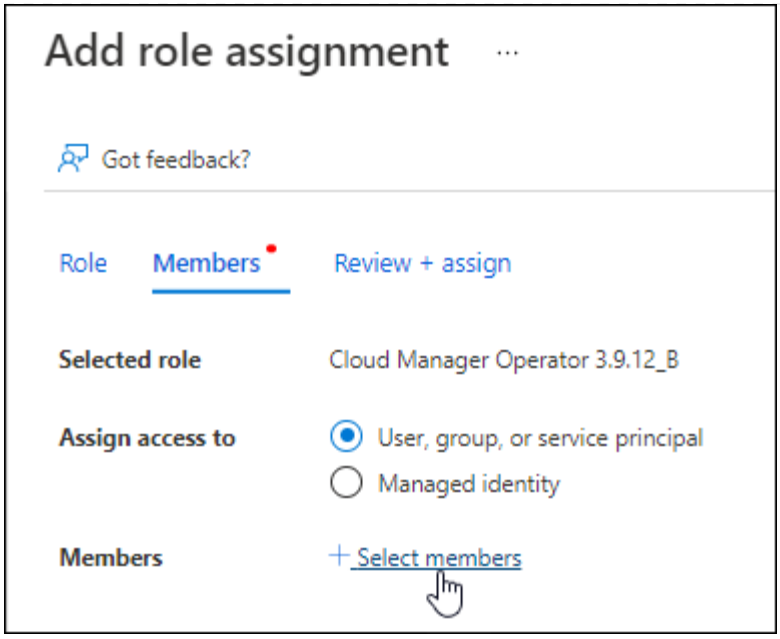
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

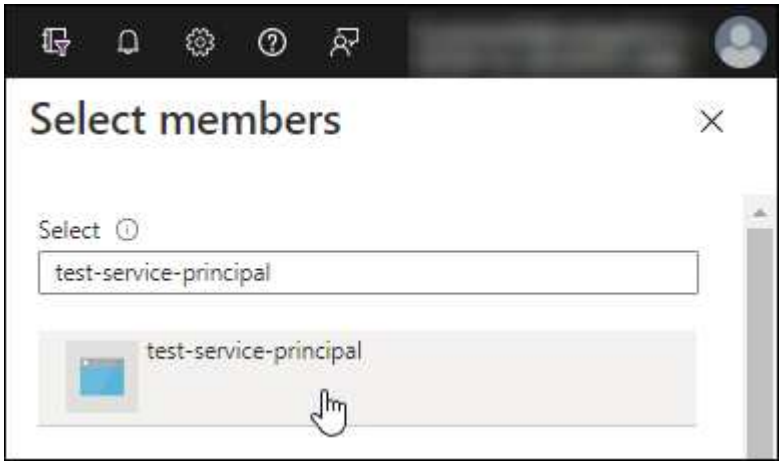
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**, realice los siguientes pasos:

      - Mantener seleccionado **Usuario, grupo o principal de servicio**.
      - Seleccione **Seleccionar miembros**.



- Busque el nombre de la aplicación.

  Veamos un ejemplo:



- Seleccione la aplicación y seleccione **Seleccionar**.
- Seleccione **Siguiente**.

f. Seleccione **revisar + asignar**.

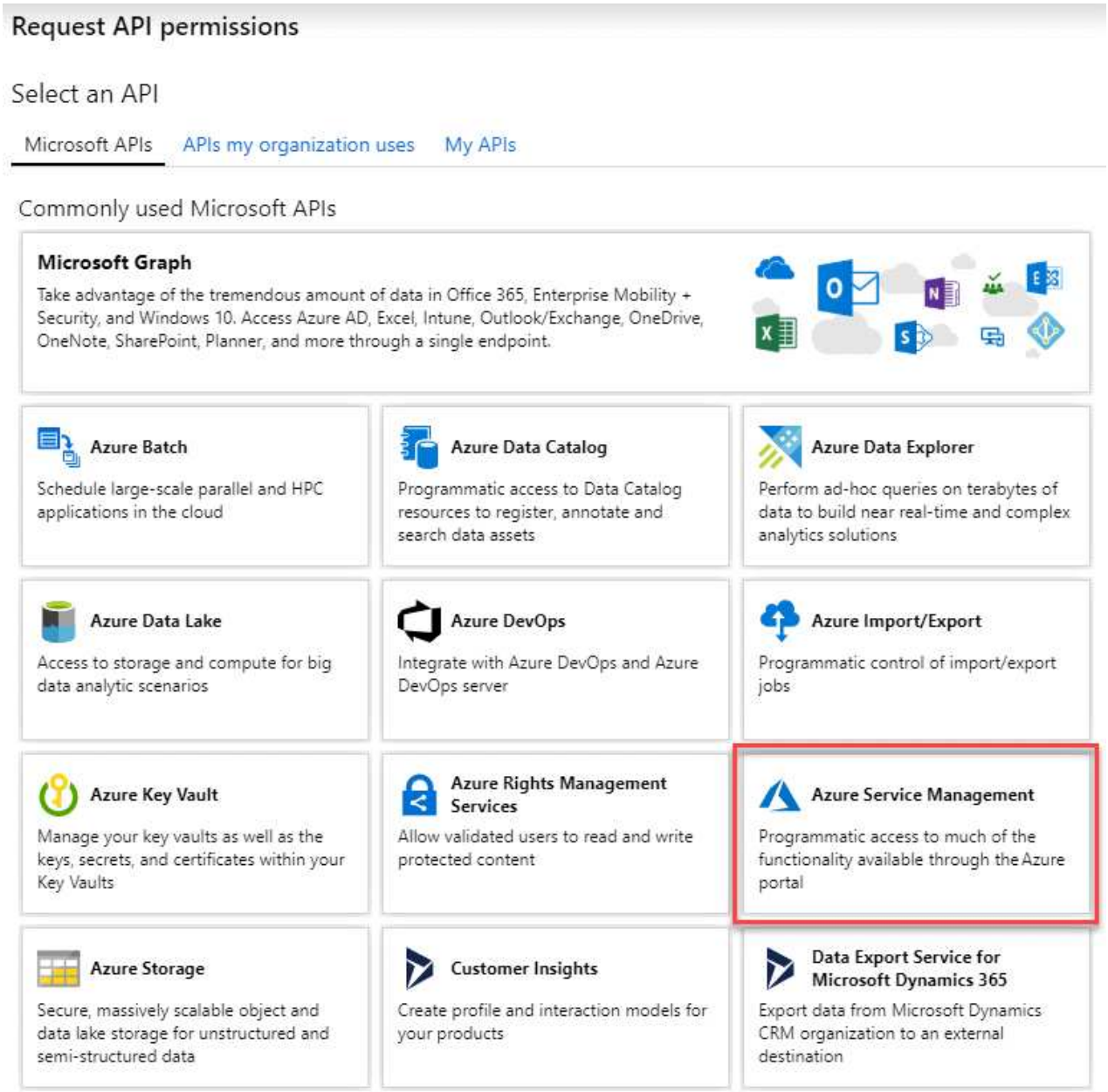
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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.

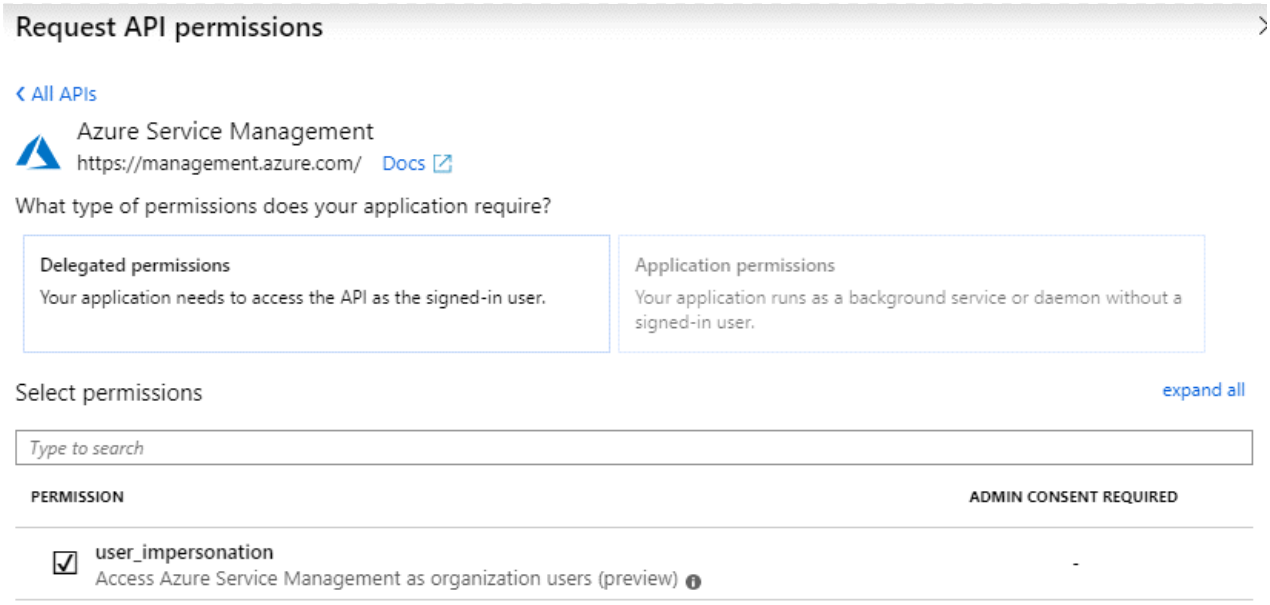
Añada permisos de API de administración de servicios de Windows Azure

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Seleccione **permisos de API > Agregar un permiso**.

3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.

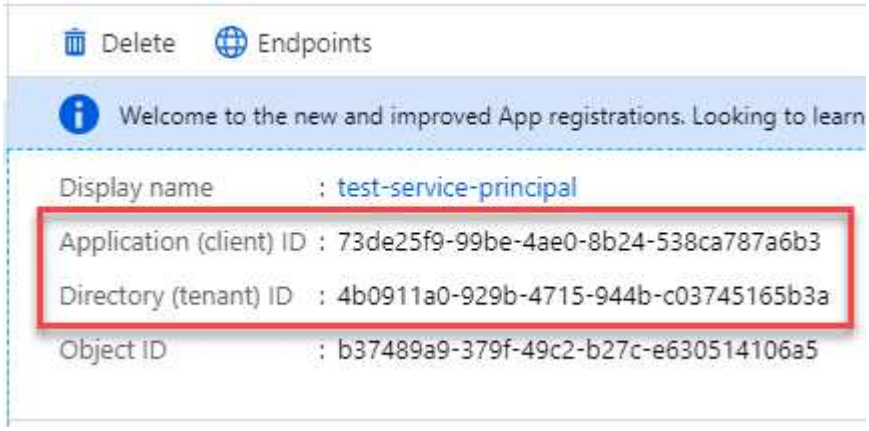


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



Obtenga el ID de aplicación y el ID de directorio de la aplicación

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Cree un secreto de cliente

1. Abra el servicio **Microsoft Entra ID**.
2. Seleccione **App registres** y seleccione su aplicación.
3. Seleccione **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copie el valor del secreto de cliente.

Ahora tienes un secreto de cliente que BlueXP puede usarlo para autenticar con Microsoft Entra ID.

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.

Cuenta de servicio de Google Cloud

Cree una función y aplíquela a una cuenta de servicio que utilizará para la instancia de Connector VM.

Pasos

1. Cree un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya los permisos definidos en "Política de conectores para Google Cloud".

   b. Desde Google Cloud, active Cloud Shell.

   c. Cargue el archivo YAML que incluye los permisos necesarios para el conector.

   d. Cree un rol personalizado mediante `gcloud iam roles create` comando.

      En el ejemplo siguiente se crea una función denominada "conector" en el nivel de proyecto:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Documentos de Google Cloud: Creación y gestión de roles personalizados"

2. Cree una cuenta de servicio en Google Cloud:

   a. En el servicio IAM y Admin, selecciona **Cuentas de servicio > Crear cuenta de servicio**.

   b. Ingrese los detalles de la cuenta de servicio y seleccione **Crear y continuar**.

   c. Seleccione la función que acaba de crear.

   d. Finalice los pasos restantes para crear la función.

      "Documentos de Google Cloud: Crear una cuenta de servicio"

Resultado

Ahora tiene una cuenta de servicio que puede asignar a la instancia de Connector VM.

Paso 6: Habilita las API de Google Cloud

Se necesitan varias API para poner en marcha Cloud Volumes ONTAP en Google Cloud.

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)
    - API del servicio de gestión de claves de cloud (KMS)

      (Solo es obligatorio si piensas utilizar el backup y la recuperación de datos de BlueXP con claves de cifrado gestionadas por el cliente (CMEK))

Despliegue el conector en modo restringido

Pon en marcha el conector en modo restringido para poder utilizar BlueXP con una conectividad saliente limitada a la capa SaaS de BlueXP. Para comenzar, instala el Connector, configura BlueXP accediendo a la interfaz de usuario que se ejecuta en el Connector y, a continuación, proporciona los permisos de nube que hayas configurado previamente.

Paso 1: Instale el conector

Instale el conector desde el mercado de su proveedor de cloud o instalando manualmente el software en su propio host Linux.

Mercado comercial AWS

Antes de empezar

Debe tener lo siguiente:

- Un VPC y una subred que cumplan los requisitos de red.

  "Obtenga información sobre los requisitos de red"

- Función IAM con una directiva adjunta que incluye los permisos necesarios para el conector.

  "Aprenda a configurar los permisos de AWS"

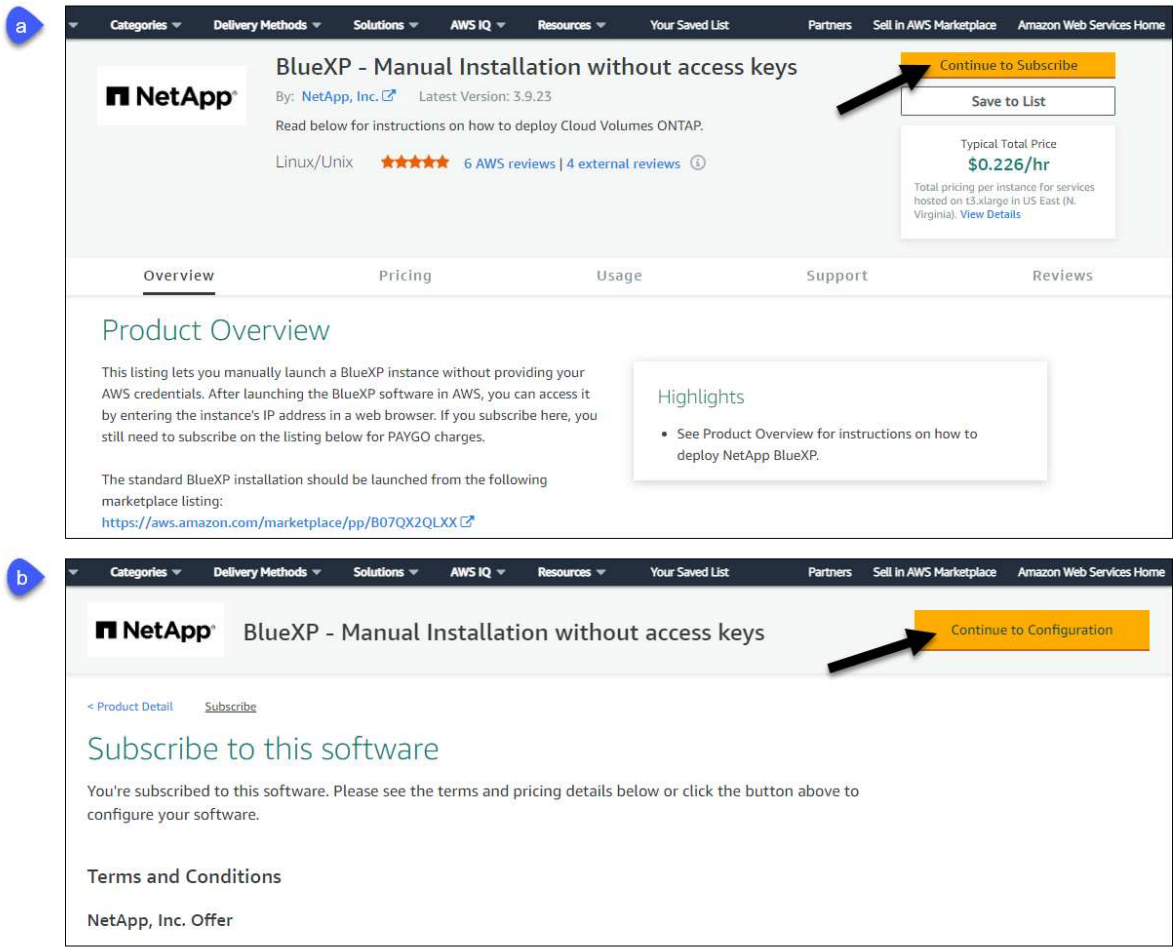
- Permisos para suscribirse y cancelar la suscripción a AWS Marketplace para su usuario de IAM.
- Comprensión de los requisitos de CPU y RAM para la instancia.

  "Revisar requisitos de instancia".

- Una pareja de claves para la instancia de EC2.

Pasos

1. Vaya a la "Página de BlueXP en AWS Marketplace"
2. En la página de Marketplace, selecciona **Continuar con la suscripción** y luego selecciona **Continuar con la configuración**.



3. Cambie cualquiera de las opciones predeterminadas y seleccione **Continuar para iniciar**.
4. En **Elegir acción**, selecciona **Iniciar a través de EC2** y luego selecciona **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**.

5. 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**: Dependiendo de la disponibilidad de la región, elija un tipo de instancia que cumpla con los requisitos de RAM y CPU (se recomienda T3.xlarge).
   - **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.

       Se requieren algunas reglas más para configuraciones específicas.

   "Ver reglas de grupos de seguridad para AWS".

   - **Configurar almacenamiento**: Mantenga el tamaño predeterminado y el tipo de disco para el volumen raíz.

     Si desea habilitar el cifrado de Amazon EBS en el volumen raíz, seleccione **Avanzado**, expanda **Volumen 1**, seleccione **Cifrado** y, a continuación, elija una clave KMS.

   - **Detalles avanzados**: En **perfil de instancia de IAM**, elija la función de IAM que incluye los permisos necesarios para el conector.
   - **Resumen**: Revisa el resumen y selecciona **Iniciar Instancia**.

Resultado

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

El futuro

Configure BlueXP.

AWS Gov Marketplace

Antes de empezar

Debe tener lo siguiente:

- Un VPC y una subred que cumplan los requisitos de red.

  "Obtenga información sobre los requisitos de red"

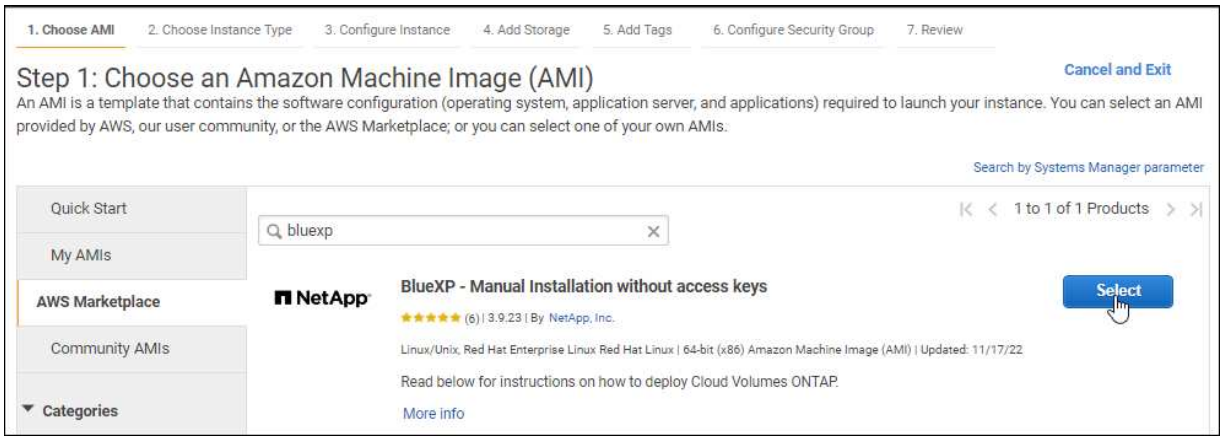
- Función IAM con una directiva adjunta que incluye los permisos necesarios para el conector.

  "Aprenda a configurar los permisos de AWS"

- Permisos para suscribirse y cancelar la suscripción a AWS Marketplace para su usuario de IAM.
- Una pareja de claves para la instancia de EC2.

Pasos

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

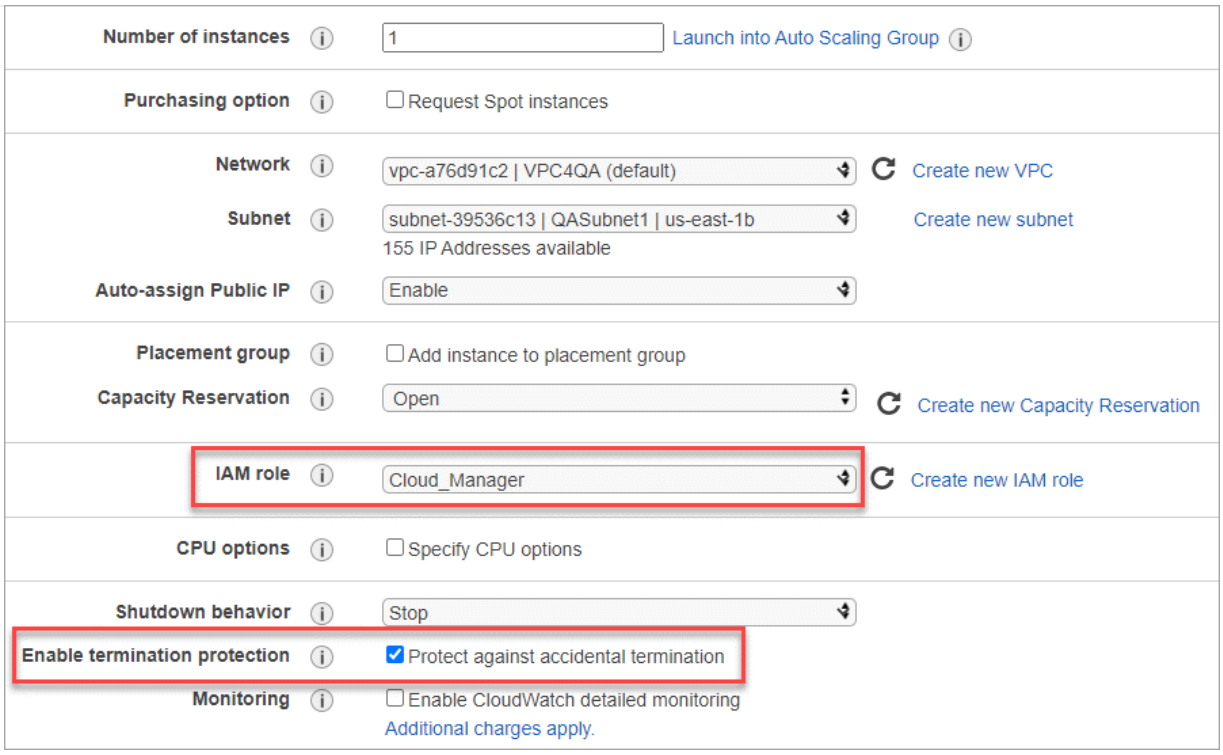


   d. Seleccione **continuar**.

2. 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.



- **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**: Revisa tus selecciones y selecciona **Lanzamiento**.

Resultado

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

El futuro

Configure BlueXP.

Azure Marketplace

Antes de empezar

Debe tener lo siguiente:

- Una red virtual y una subred que cumplan los requisitos de red.

  "Obtenga información sobre los requisitos de red"

- Una función personalizada de Azure que incluye los permisos necesarios para el conector.

  "Aprenda a configurar los permisos de Azure"

Pasos

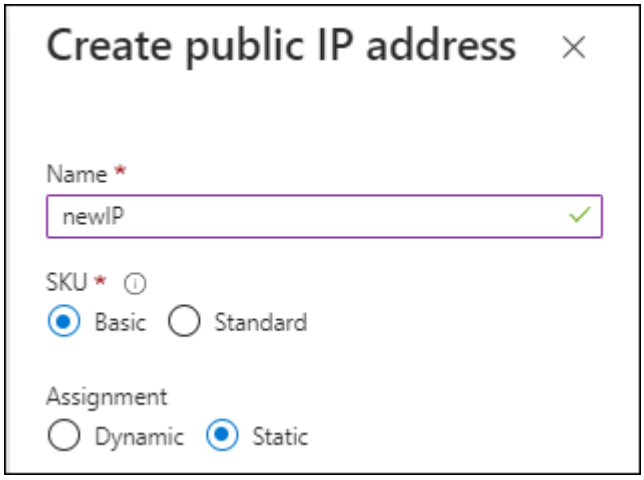
1. Vaya a la página NetApp Connector VM del Azure Marketplace.
   - "Página de Azure Marketplace para regiones comerciales"

- "Página de Azure Marketplace para regiones gubernamentales de Azure"

2. Selecciona **Obtenlo ahora** y luego selecciona **Continuar**.
3. Desde el portal de Azure, seleccione **Crear** y siga los pasos para configurar la máquina virtual.

   Tenga en cuenta lo siguiente al configurar la máquina virtual:

   - **VM size**: Elija un tamaño de VM que cumpla con los requisitos de CPU y RAM. Recomendamos DS3 v2.
   - **Discos**: El conector puede funcionar de forma óptima con discos HDD o SSD.
   - **IP pública**: Si desea utilizar una dirección IP pública con el conector VM, la dirección IP debe utilizar un SKU básico para garantizar que BlueXP utilice esta dirección IP pública.



     Si en su lugar utiliza una dirección IP de SKU estándar, BlueXP utiliza la dirección *private* IP del conector, en lugar de la dirección IP pública. Si el equipo que está utilizando para acceder a la consola BlueXP no tiene acceso a esa dirección IP privada, las acciones de la consola BlueXP fallarán.

   "Documentación para Azure: SKU de IP pública"

   - **Grupo de seguridad de red**: El conector requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

     "Ver reglas de grupo de seguridad para Azure".

   - **Identidad**: En **Gestión**, seleccione **Activar identidad administrada asignada por el sistema**.

     Esta configuración es importante porque una identidad administrada permite que la máquina virtual Connector se identifique con Microsoft Entra ID sin proporcionar credenciales. "Obtenga más información sobre las identidades gestionadas para recursos de Azure".

4. En la página **Review + create**, revise sus selecciones y seleccione **Create** para iniciar la implementación.

Resultado

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.

El futuro

Configure BlueXP.

Instalación manual

Antes de empezar

Debe tener lo siguiente:

- 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.

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

  Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

- Un certificado firmado por CA, si el servidor proxy utiliza HTTPS o si el proxy es un proxy de interceptación.

Acerca de esta tarea

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 "en línea" del conector que se utiliza en su red o en la nube. Hay disponible un instalador "sin conexión" independiente para el conector, pero sólo es compatible con implementaciones en modo privado.

4. Asigne permisos para ejecutar el script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

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

5. Ejecute el script de instalación.

```
./BlueXP-Connector-Cloud-<version> --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:

```
./BlueXP-Connector-Cloud-v3.9.38 --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://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Tenga en cuenta lo siguiente:

  - El usuario puede ser un usuario local o un usuario de dominio.
  - Para un usuario de dominio, debe utilizar el código ASCII para \ como se muestra anteriormente.
  - BlueXP no admite contraseñas que incluyan el carácter @.

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

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.

El futuro

Configure BlueXP.

Paso 2: Configura BlueXP

Cuando acceda a la consola BlueXP por primera vez, se le solicitará que elija una cuenta para asociar el conector y tendrá que activar el modo restringido.

Si ya tiene una cuenta y desea crear otra, debe utilizar la API de soporte. "Aprenda a crear una cuenta de BlueXP adicional".

Pasos

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. Regístrese o inicie sesión en BlueXP.
3. Después de iniciar sesión, configure BlueXP:

   a. Introduzca un nombre para el conector.

   b. Introduzca un nombre para una nueva cuenta de BlueXP o seleccione una cuenta existente.

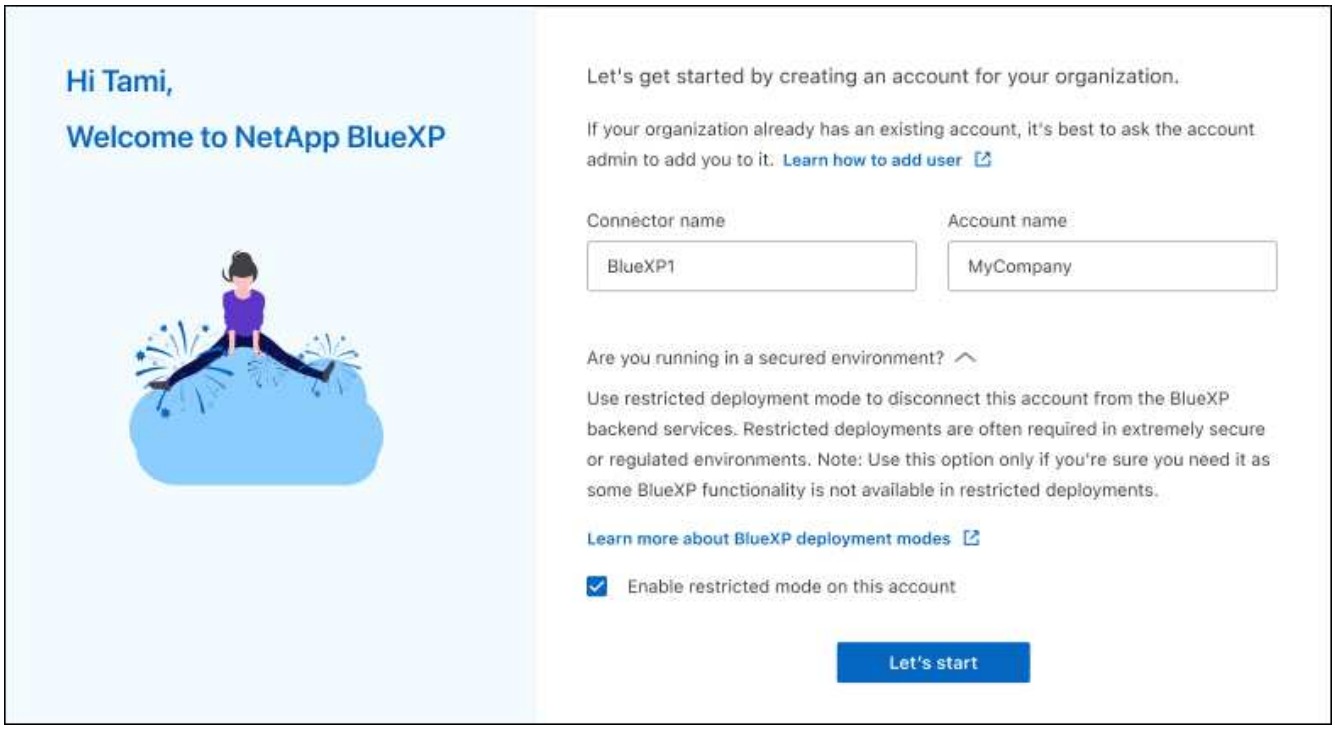
      Puede seleccionar una cuenta existente si su inicio de sesión ya está asociado con una cuenta de BlueXP.

   c. Seleccione **¿está ejecutando en un entorno protegido?**

   d. Seleccione **Activar modo restringido en esta cuenta**.

      Tenga en cuenta que no puede cambiar esta configuración después de que BlueXP cree la cuenta. No se puede activar el modo restringido más adelante y no se puede desactivar más adelante.

      Si ha desplegado el conector en una región gubernamental, la casilla de verificación ya está activada y no se puede cambiar. Esto se debe a que el modo restringido es el único modo compatible con las regiones gubernamentales.



   a. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y configurado con su cuenta BlueXP. Todos los usuarios deben acceder a BlueXP mediante la dirección IP de la instancia de Connector.

El futuro

Proporcione a BlueXP los permisos que configuró anteriormente.

Paso 3: Proporcionar permisos a BlueXP

Si implementó el conector desde Azure Marketplace o si instaló manualmente el software Connector, debe proporcionar los permisos que configuró anteriormente para poder utilizar los servicios de BlueXP.

Estos pasos no se aplican si ha implementado el conector desde AWS Marketplace porque ha elegido el rol de IAM necesario durante la implementación.

"Aprenda cómo preparar los permisos en el cloud".

Rol IAM de AWS

Conecte el rol IAM que ha creado previamente a la instancia de EC2 donde ha instalado Connector.

Estos pasos sólo se aplican si instaló manualmente el conector en AWS. En el caso de implementaciones de AWS Marketplace, ya ha asociado la instancia del conector con una función IAM que incluye los permisos necesarios.

Pasos

1. Vaya a la consola de Amazon EC2.
2. Seleccione **instancias**.
3. Seleccione la instancia de conector.
4. Seleccione **acciones > Seguridad > Modificar función IAM**.
5. Seleccione el rol de IAM y seleccione **Actualizar rol de IAM**.

Resultado

BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

Clave de acceso de AWS

Proporcione a BlueXP la clave de acceso de AWS para un usuario de IAM que tenga los permisos necesarios.

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Servicios Web de Amazon > conector**.
   b. **Definir credenciales**: Introduzca una clave de acceso y una clave secreta de AWS.
   c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.
   d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

Rol de Azure

Vaya al portal de Azure y asigne el rol personalizado de Azure a la máquina virtual Connector para una o más suscripciones.

Pasos

1. En el Portal de Azure, abra el servicio **Suscripciones** y seleccione su suscripción.

   Es importante asignar el rol desde el servicio **Suscripciones** porque especifica el alcance de la

asignación de rol en el nivel de suscripción. El *scope* define el juego de recursos al que se aplica el acceso. Si especifica un ámbito a otro nivel (por ejemplo, a nivel de máquina virtual), se verá afectada su capacidad para completar acciones desde BlueXP.

"Documentación de Microsoft Azure: Conozca el ámbito de control de acceso basado en roles de Azure"

2. Selecciona **Control de acceso (IAM)** > **Añadir** > **Añadir asignación de rol**.
3. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **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.

4. En la ficha **Miembros**, realice los siguientes pasos:
   a. Asignar acceso a una **identidad administrada**.
   b. Seleccione **Seleccionar miembros**, seleccione la suscripción en la que se creó la máquina virtual Connector, en **Identidad administrada**, elija **Máquina virtual** y, a continuación, seleccione la máquina virtual Connector.
   c. Selecciona **Seleccionar**.
   d. Seleccione **Siguiente**.
   e. Seleccione **revisar + asignar**.
   f. Si desea administrar recursos en suscripciones adicionales de Azure, cambie a esa suscripción y repita estos pasos.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Servicio principal de Azure

Proporcione a BlueXP las credenciales para la entidad de servicio de Azure que configuró anteriormente.

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.
   b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:
      - ID de aplicación (cliente)
      - ID de directorio (inquilino)
      - Secreto de cliente
   c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Cuenta de servicio de Google Cloud

Asocie la cuenta de servicio a la máquina virtual del conector.

Pasos

1. Vaya al portal de Google Cloud y asigne la cuenta de servicio a la instancia de Connector VM.

   "Documentación de Google Cloud: Cambiar la cuenta de servicio y los ámbitos de acceso para una instancia"

2. Si quieres gestionar recursos en otros proyectos, otorga acceso agregando la cuenta de servicio con el rol BlueXP a ese proyecto. Deberá repetir este paso con cada proyecto.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Google Cloud en su nombre.

Suscribirse a BlueXP (modo restringido)

Suscríbase a BlueXP en el mercado de su proveedor de la nube para pagar los servicios de BlueXP a una tarifa por hora (PAYGO) o a través de un contrato anual. Si adquirió una licencia de NetApp (BYOL), también deberá suscribirse a la oferta de mercado. Su licencia siempre se cobra primero, pero se le cobrará la tarifa por hora si excede la capacidad de su licencia o si el plazo de la licencia expira.

Una suscripción al mercado permite cargar los siguientes servicios de BlueXP con modo restringido:

- Backup y recuperación
- Clasificación
- Cloud Volumes ONTAP

Antes de empezar

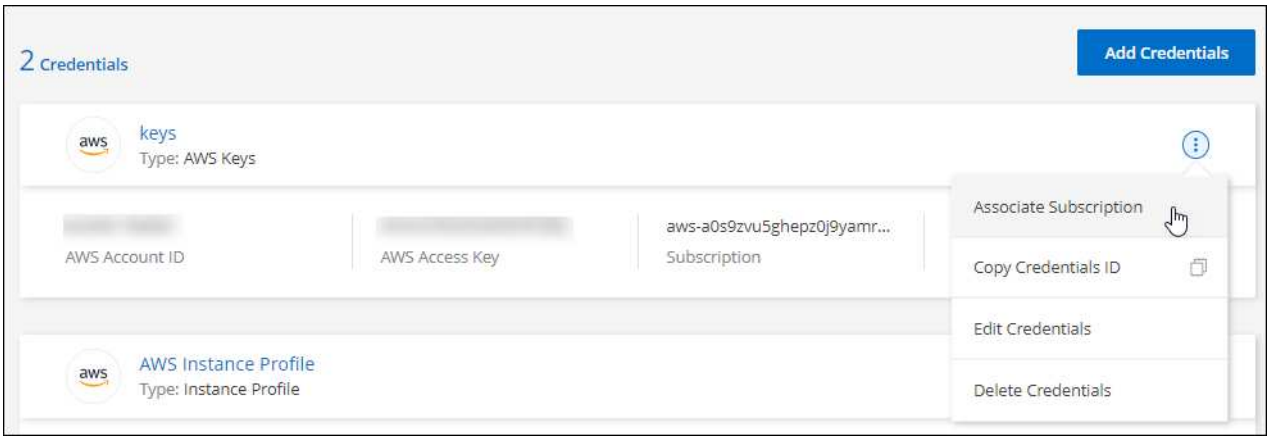
La suscripción a BlueXP implica asociar una suscripción al mercado con las credenciales de la nube asociadas con un conector. Si ha seguido el flujo de trabajo de inicio con modo restringido, ya debe tener un conector. Para obtener más información, consulte la "Inicio rápido para BlueXP en modo restringido".

AWS

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y seleccione **asociado**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos del AWS Marketplace:

   a. Seleccione **Ver opciones de compra**.

   b. Seleccione **Suscribirse**.

   c. Seleccione **Configurar su cuenta**.

      Se le redirigirá al sitio web de BlueXP.

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

      - Seleccione las cuentas de BlueXP con 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.

      - Seleccione **Guardar**.

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

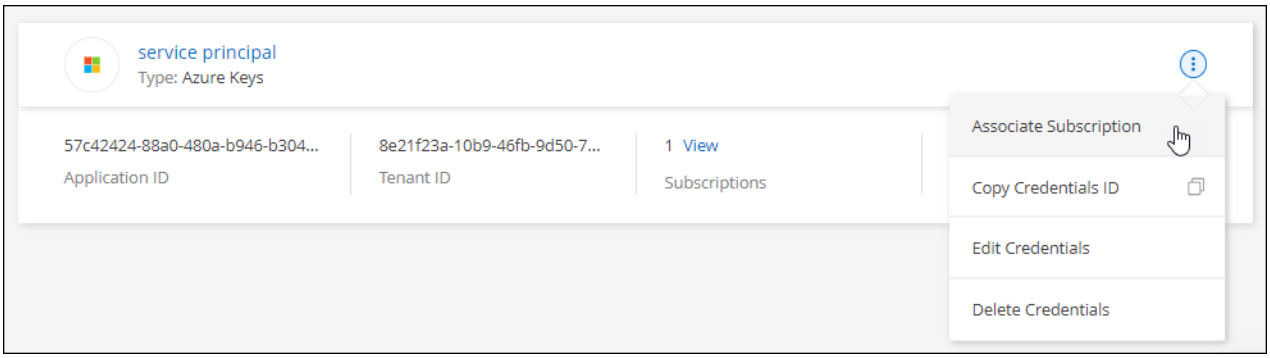
Suscríbete a BlueXP desde AWS Marketplace

Azure

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y seleccione **asociado**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos de Azure Marketplace:

   a. Si se le solicita, inicie sesión en su cuenta de Azure.

   b. Seleccione **Suscribirse**.

   c. Rellene el formulario y seleccione **Suscribirse**.

   d. Una vez completado el proceso de suscripción, seleccione **Configurar cuenta ahora**.

      Se le redirigirá al sitio web de BlueXP.

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

      - Seleccione las cuentas de BlueXP con 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.

      - Seleccione **Guardar**.

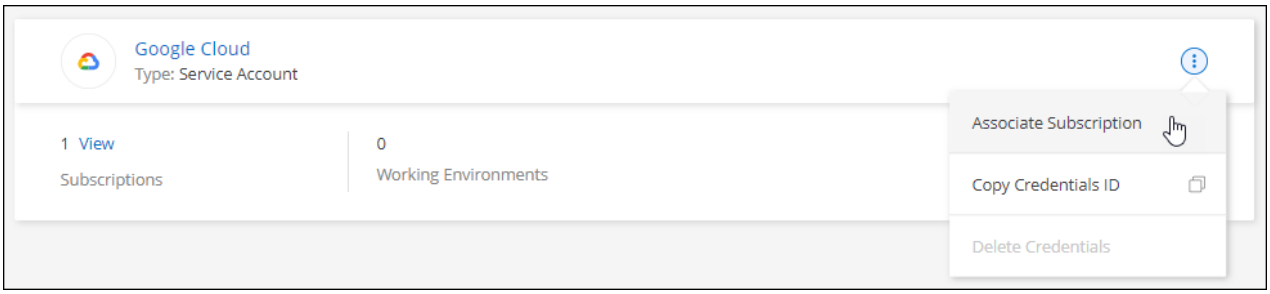
        En el siguiente vídeo se muestran los pasos para suscribirse desde Azure Marketplace:

Suscríbete a BlueXP desde Azure Marketplace

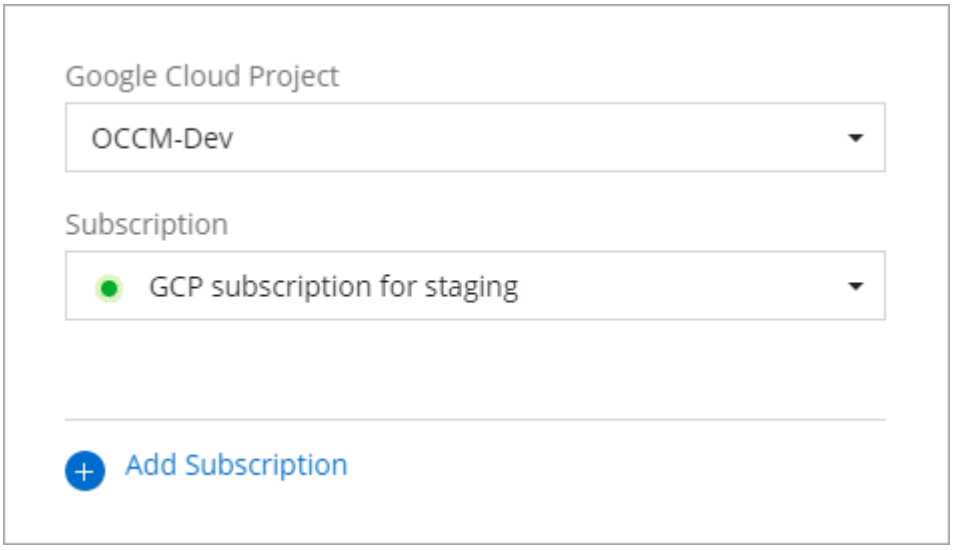
Google Cloud

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.



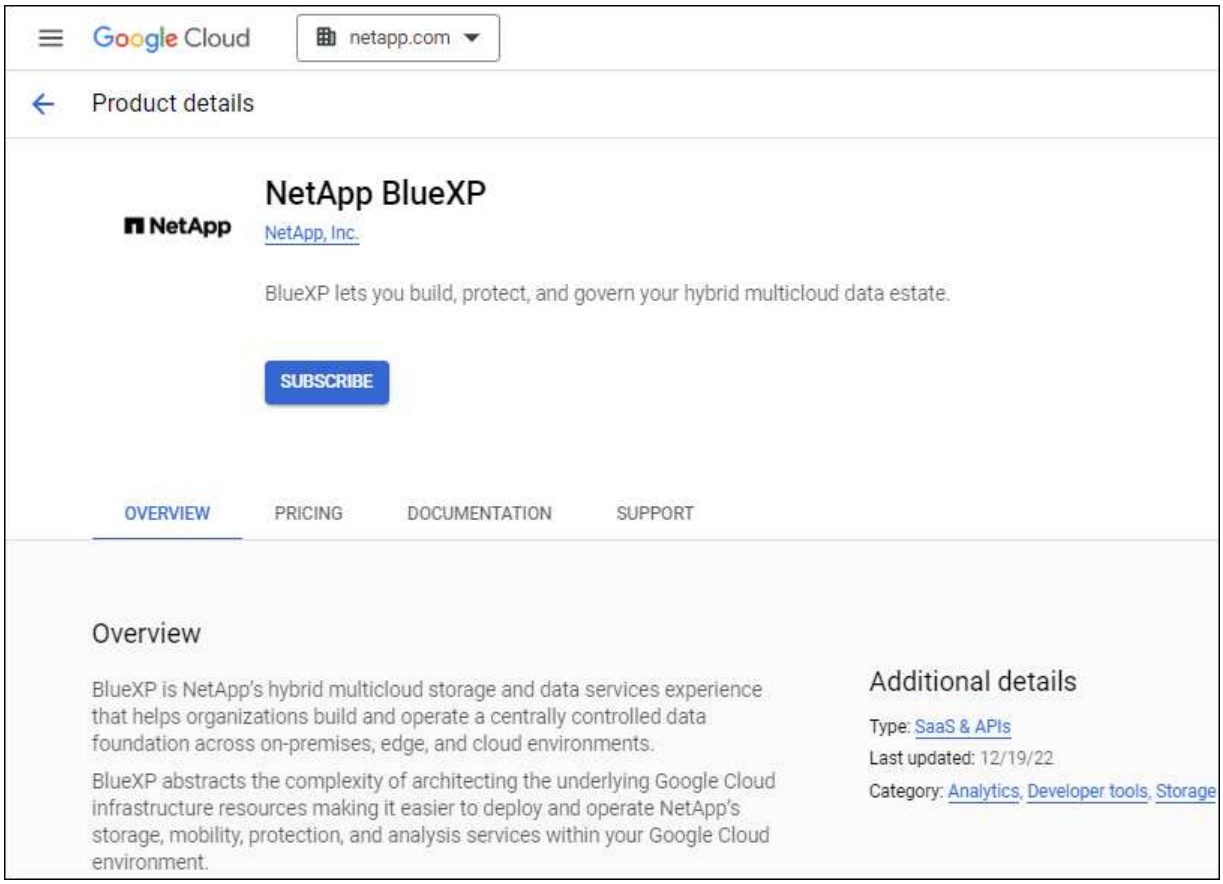
3. Para asociar las credenciales a una suscripción existente, seleccione un proyecto de Google Cloud y una suscripción en la lista desplegable y, a continuación, seleccione **asociado**.



4. Si aún no tiene una suscripción, seleccione **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.



b. Seleccione **Suscribirse**.

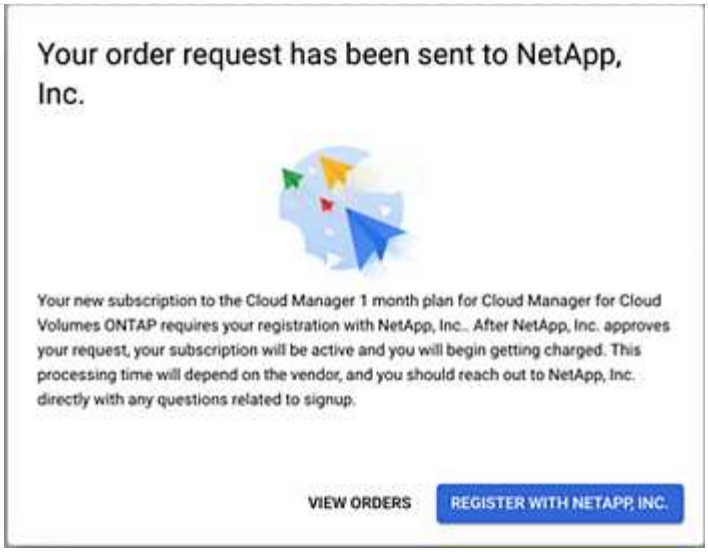
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.

d. Seleccione **Suscribirse**.

   Este paso envía la solicitud de transferencia a NetApp.

e. En el cuadro de diálogo emergente, seleccione **Registro con NetApp, Inc.**

   Este paso debe completarse para vincular la suscripción a Google Cloud a su cuenta de BlueXP. 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 BlueXP con 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.

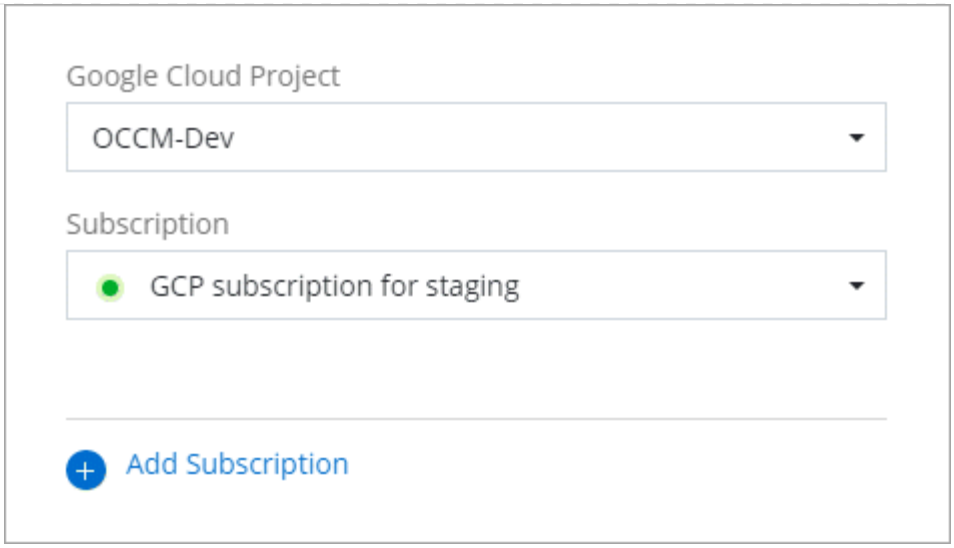
Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

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

Suscríbete a BlueXP desde Google Cloud Marketplace

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



Enlaces relacionados

- "Gestione las licencias basadas en la capacidad de su propia licencia para Cloud Volumes ONTAP"
- "Gestiona las licencias BYOL para los servicios de datos de BlueXP"
- "Gestione las credenciales y suscripciones de AWS para BlueXP"
- "Gestione credenciales y suscripciones de Azure para BlueXP"
- "Administrar las credenciales y suscripciones de Google Cloud para BlueXP"

Qué puede hacer después (modo restringido)

Después de empezar a utilizar BlueXP en modo restringido, puede empezar a utilizar los servicios BlueXP compatibles con modo restringido.

Para obtener ayuda, consulte la documentación de estos servicios:

- "Documentos de Amazon FSX para ONTAP"
- "Documentos de Azure NetApp Files"
- "Documentos de backup y recuperación"
- "Documentos de clasificación"
- "Documentos de Cloud Volumes ONTAP"
- "Documentos del clúster ONTAP en las instalaciones"
- "Documentos de replicación"

Enlace relacionado

"Modos de implementación de BlueXP"

Comience con el modo privado

Flujo de trabajo inicial (modo privado)

Empieza a usar BlueXP en modo privado preparando tu entorno y poniendo en marcha Connector.

El modo privado se suele utilizar con entornos locales que no tienen conexión a Internet y con regiones de nube seguras, lo que incluye "Cloud secreto de AWS", "Cloud secreto principal de AWS", y. "Azure IL6"

Antes de empezar, debería comprender "Cuentas BlueXP", "Conectores", y. "modos de despliegue".

1 **"Prepárese para la puesta en marcha"**

1. Prepare un host de Linux dedicado que cumpla los requisitos de CPU, RAM, espacio en disco, Docker Engine y mucho más.
2. Configure las redes que proporcionen acceso a las redes de destino.
3. Para implementaciones en la nube, configure permisos en su proveedor de cloud para que pueda asociar dichos permisos con el conector después de instalar el software.

2 **"Despliegue el conector"**

1. Instale el software del conector en su propio host Linux.
2. Configure BlueXP abriendo un navegador Web e introduciendo la dirección IP del host Linux.
3. Para implementaciones en la nube, proporcione a BlueXP los permisos que configuró anteriormente.

Preparación para la implementación en modo privado

Prepara tu entorno antes de poner en marcha BlueXP en modo privado. Por ejemplo, debe revisar los requisitos del host, preparar redes, configurar permisos y mucho más.

> Si desea utilizar BlueXP en "Cloud secreto de AWS" o la "Cloud secreto principal de AWS", entonces debe seguir instrucciones separadas para comenzar en esos entornos. "Descubra cómo empezar a utilizar Cloud Volumes ONTAP en el cloud secreto de AWS o en el cloud secreto superior"

Paso 1: Entender cómo funciona el modo privado

Antes de empezar, debe comprender cómo funciona BlueXP en modo privado.

Por ejemplo, debe entender que necesita utilizar la interfaz basada en explorador que está disponible localmente desde el conector BlueXP que necesita instalar. No puede acceder a BlueXP desde la consola basada en Web que se proporciona a través de la capa SaaS.

Además, no todos los servicios de BlueXP están disponibles.

"Aprenda cómo funciona el modo privado".

Paso 2: Revise las opciones de instalación

En modo privado, puede instalar el conector en las instalaciones o en la nube mediante la instalación manual

del conector en su propio host Linux.

Si desea crear un sistema de Cloud Volumes ONTAP en Google Cloud, el conector debe estar en ejecución en Google Cloud y no puede ejecutarse en las instalaciones.

Paso 3: Revise 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.

Host dedicado

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

Sistemas operativos compatibles

- Sistema operativo Ubuntu 22,04 LTS
- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7,6, 7,7, 7,8 y 7,9

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

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

Hipervisor

Se requiere un hipervisor con configuración básica o alojado certificado para ejecutar Ubuntu, CentOS o Red Hat Enterprise Linux.

"Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"

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 de Google Cloud

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"

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 en el host antes de instalar Connector.

- La versión mínima admitida es 19,3.1.
- La versión máxima admitida es 25,0.5.

"Ver las instrucciones de instalación"

Paso 4: Prepare la red para el conector

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.

Conexiones a redes de destino

El conector debe tener una conexión de red a la ubicación en la que desea gestionar el almacenamiento. Por ejemplo, el VPC o vnet donde planea poner en marcha Cloud Volumes ONTAP, o el centro de datos donde residen los clústeres de ONTAP en las instalaciones.

Extremos para operaciones del día a día

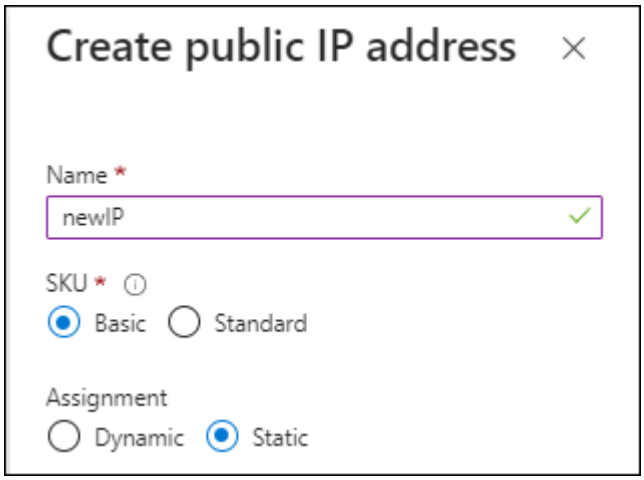
Connector se pone en contacto con los siguientes puntos finales para gestionar los recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Para administrar recursos en la región de Azure IL6.

Puntos finales	Específico
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://www.googleapis.com/compute/v1/ https://compute.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.

La dirección IP pública en Azure

Si desea utilizar una dirección IP pública con Connector VM en Azure, la dirección IP debe utilizar una SKU básica para garantizar que BlueXP utilice esta dirección IP pública.



Si en su lugar utiliza una dirección IP de SKU estándar, BlueXP utiliza la dirección *private* IP del conector, en lugar de la dirección IP pública. Si el equipo que está utilizando para acceder a la consola BlueXP no tiene acceso a esa dirección IP privada, las acciones de la consola BlueXP fallarán.

"Documentación para Azure: SKU de IP pública"

Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación.

- Dirección IP
- Credenciales
- Certificado HTTPS

Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

+
Con el modo privado, la única vez que BlueXP envía tráfico saliente es al proveedor de cloud para crear un sistema Cloud Volumes ONTAP.

Puertos

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

HTTP (80) y HTTPS (443) proporcionan acceso a la consola BlueXP. SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.

Habilite NTP

Si tienes pensado utilizar la clasificación de BlueXP para analizar tus orígenes de datos corporativos, debes habilitar un servicio de protocolo de tiempo de redes (NTP) tanto en el sistema BlueXP Connector como en el sistema de clasificación de BlueXP para que el tiempo se sincronice entre los sistemas. "Más información sobre la clasificación de BlueXP"

Paso 5: Preparar permisos en la nube

Si está considerando crear sistemas Cloud Volumes ONTAP, BlueXP requiere permisos de su proveedor de cloud. Debe configurar permisos en su proveedor de cloud y, a continuación, asociar dichos permisos a la instancia de conector después de instalarla.

Para ver los pasos requeridos, seleccione la opción de autenticación que desee usar para su proveedor de cloud.

Si va a instalar el conector en las instalaciones, debe proporcionar permisos con claves de acceso de AWS o un director de servicio de Azure. No se admiten las demás opciones.

Rol IAM de AWS

Utilice un rol de IAM para proporcionar al conector permisos. Deberá asociar manualmente el rol a la instancia de EC2 del conector.

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:
   a. Selecciona **Políticas > Crear política**.
   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".
   c. Finalice los pasos restantes para crear la directiva.
3. Cree un rol IAM:
   a. Selecciona **Roles > Crear rol**.
   b. Seleccione **Servicio AWS > EC2**.
   c. Agregue permisos asociando la directiva que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

Resultado

Ahora tiene un rol de IAM para la instancia de Connector EC2.

Clave de acceso de AWS

Configurar permisos y una clave de acceso para un usuario de IAM. Deberá proporcionar a BlueXP la clave de acceso de AWS después de instalar el conector y configurar BlueXP.

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:
   a. Selecciona **Políticas > Crear política**.
   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".
   c. Finalice los pasos restantes para crear la directiva.

      Dependiendo de los servicios de BlueXP que tenga previsto utilizar, puede que necesite crear una segunda política.

   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. "Obtenga más información sobre las políticas de IAM para el conector".

3. Adjunte las políticas a un usuario de IAM.
   - "Documentación de AWS: Crear roles de IAM"
   - "Documentación de AWS: Adición y eliminación de políticas de IAM"
4. Asegúrese de que el usuario tiene una clave de acceso que puede agregar a BlueXP después de instalar el conector.

Resultado

La cuenta ahora tiene los permisos necesarios.

Rol de Azure

Cree un rol personalizado de Azure con los permisos necesarios. Asignará este rol al conector VM.

Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

Pasos

1. Habilite una identidad administrada asignada por el sistema en la máquina virtual donde tenga pensado instalar el conector de modo que pueda proporcionar los permisos de Azure necesarios a través de una función personalizada.

   "Documentación de Microsoft Azure: Configure las identidades gestionadas para los recursos de Azure en una máquina virtual mediante el portal de Azure"

2. Copie el contenido de "Permisos de función personalizada para el conector" Y guárdelos en un archivo JSON.
3. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

   Debes añadir el ID de cada suscripción de Azure que quieras utilizar con BlueXP.

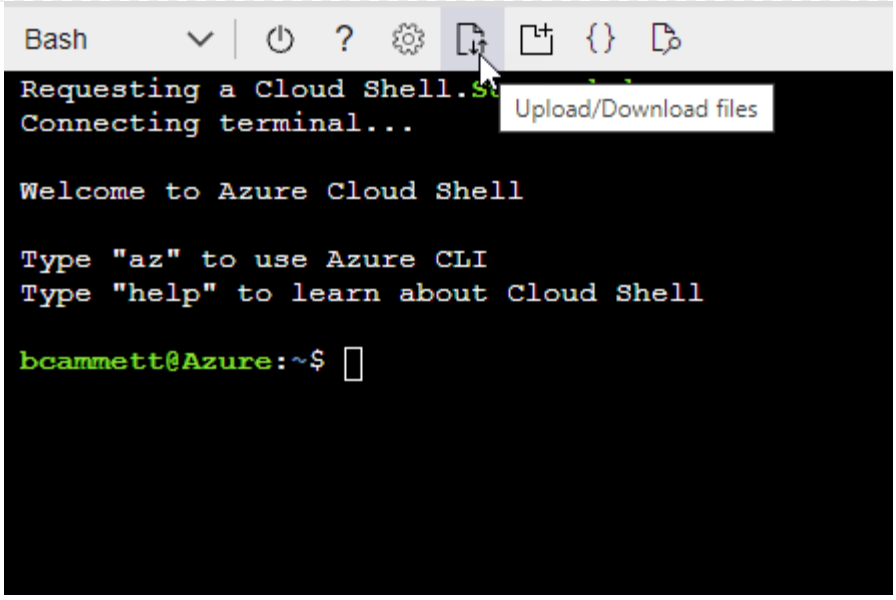
   ejemplo

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

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

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

Resultado

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

Servicio principal de Azure

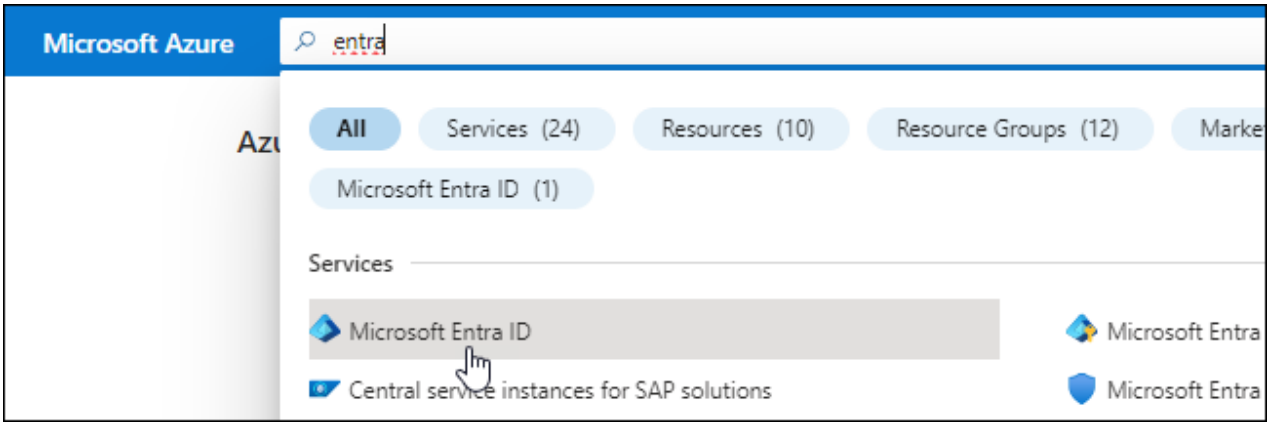
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita. Necesitará proporcionar estas credenciales a BlueXP después de instalar el conector y configurar BlueXP.

Cree una aplicación Microsoft Entra para el control de acceso basado en roles

1. Asegúrese de tener permisos en Azure para crear una aplicación de Active Directory y para asignar la aplicación a un rol.

   Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios"

2. Desde el portal de Azure, abra el servicio **Microsoft Entra ID**.



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. 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.
6. Seleccione **Registrar**.

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

   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.

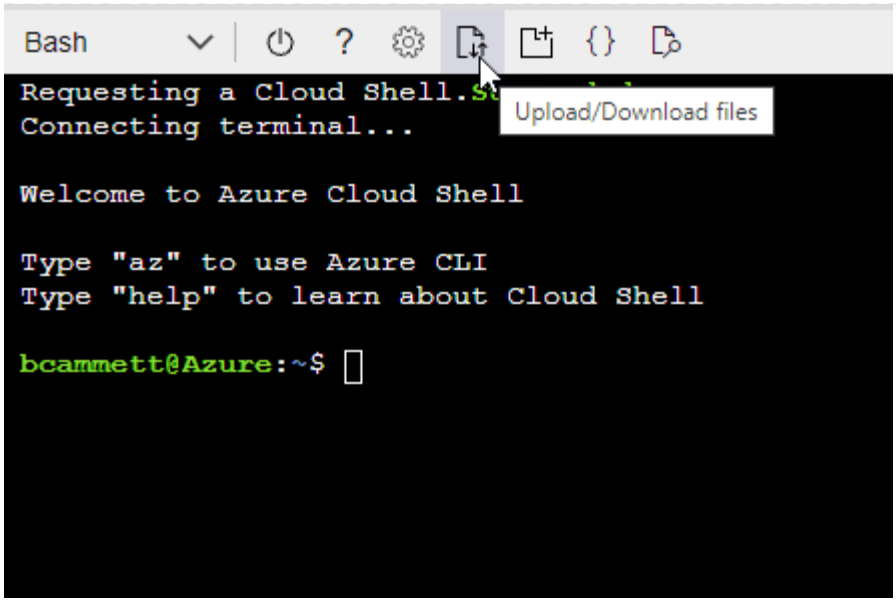
      ejemplo

      ```
      "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:

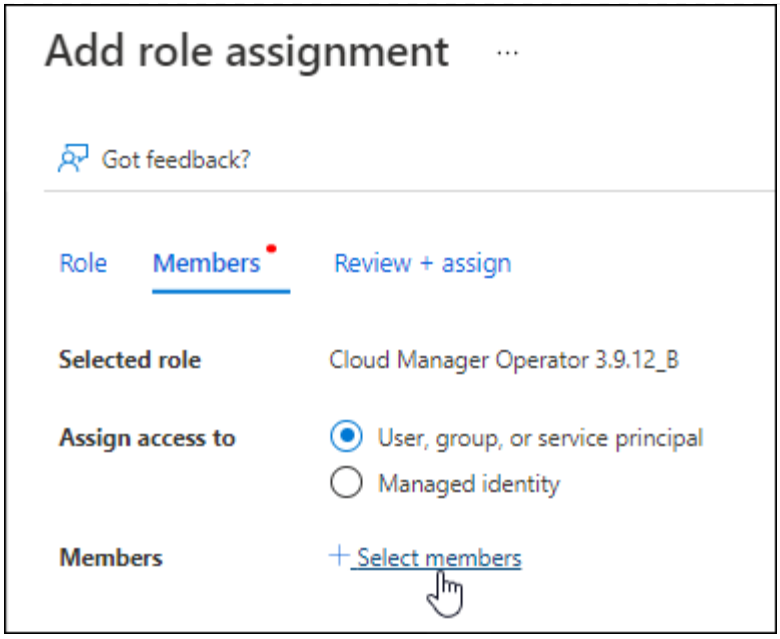
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

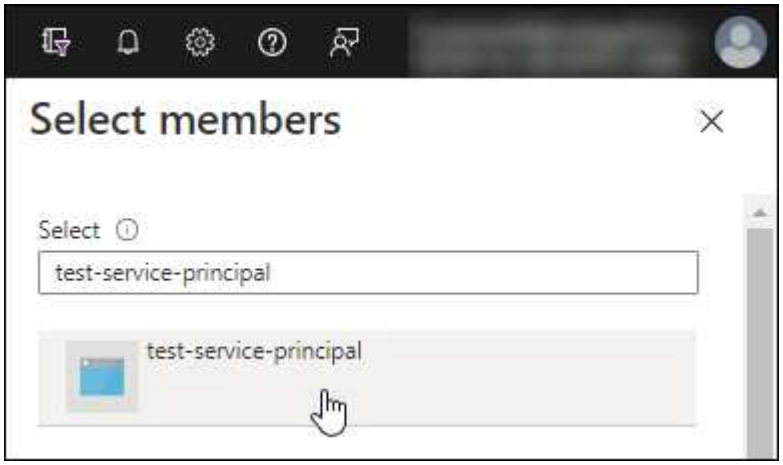
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**, realice los siguientes pasos:

      - Mantener seleccionado **Usuario, grupo o principal de servicio**.
      - Seleccione **Seleccionar miembros**.



- Busque el nombre de la aplicación.

  Veamos un ejemplo:



- Seleccione la aplicación y seleccione **Seleccionar**.
- Seleccione **Siguiente**.

f. Seleccione **revisar + asignar**.

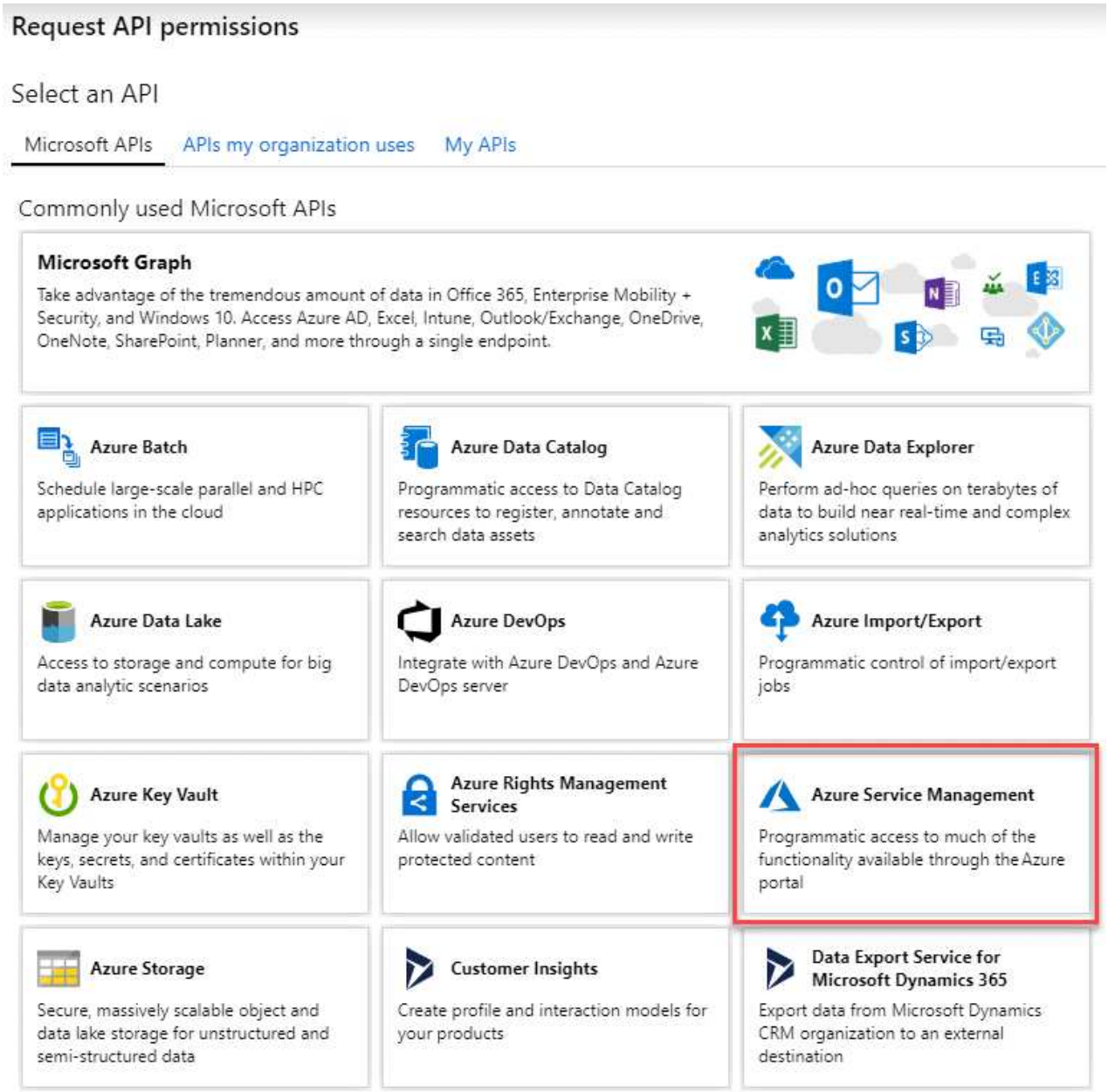
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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.

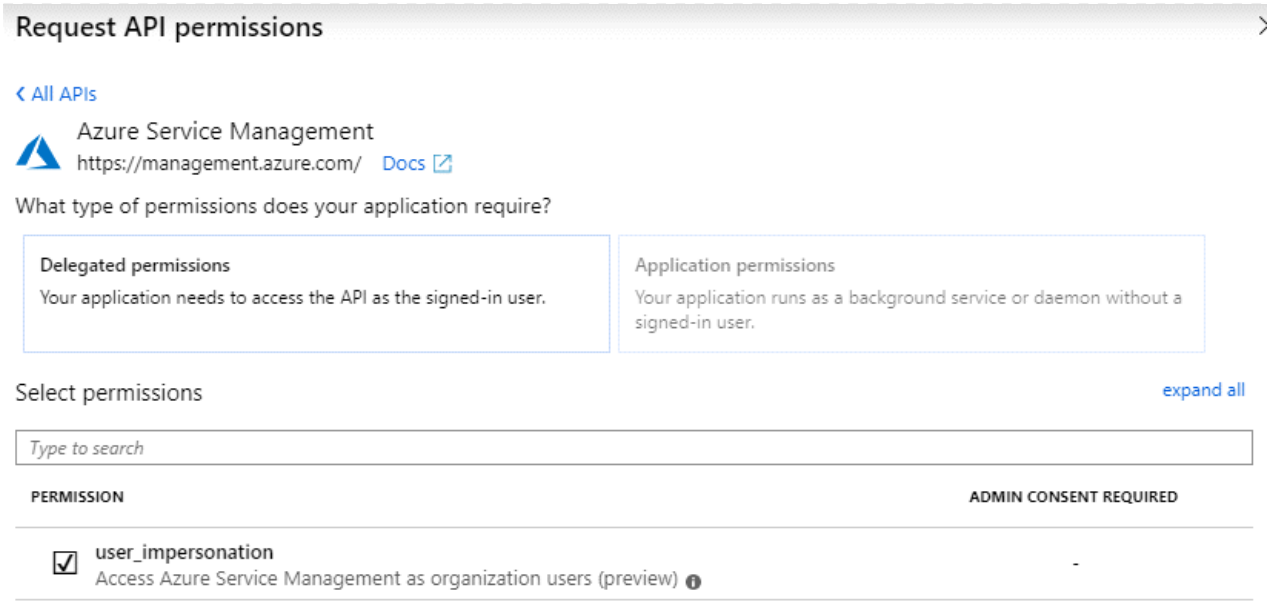
Añada permisos de API de administración de servicios de Windows Azure

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Seleccione **permisos de API > Agregar un permiso**.

3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.

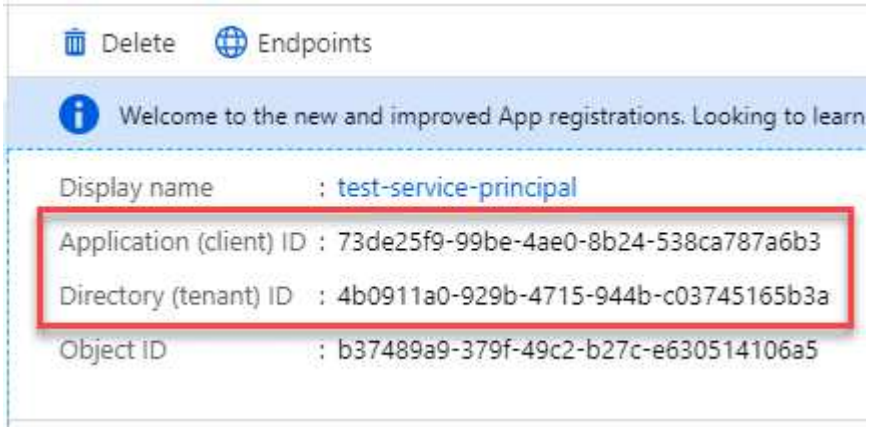


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



Obtenga el ID de aplicación y el ID de directorio de la aplicación

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Cree un secreto de cliente

1. Abra el servicio **Microsoft Entra ID**.
2. Seleccione **App registres** y seleccione su aplicación.
3. Seleccione **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copie el valor del secreto de cliente.

Ahora tienes un secreto de cliente que BlueXP puede usarlo para autenticar con Microsoft Entra ID.

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.

Cuenta de servicio de Google Cloud

Cree una función y aplíquela a una cuenta de servicio que utilizará para la instancia de Connector VM.

Pasos

1. Cree un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya los permisos definidos en "Política de conectores para Google Cloud".

   b. Desde Google Cloud, active Cloud Shell.

   c. Cargue el archivo YAML que incluye los permisos necesarios para el conector.

   d. Cree un rol personalizado mediante `gcloud iam roles create` comando.

      En el ejemplo siguiente se crea una función denominada "conector" en el nivel de proyecto:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Documentos de Google Cloud: Creación y gestión de roles personalizados"

2. Cree una cuenta de servicio en Google Cloud:

   a. En el servicio IAM y Admin, selecciona **Cuentas de servicio > Crear cuenta de servicio**.

   b. Ingrese los detalles de la cuenta de servicio y seleccione **Crear y continuar**.

   c. Seleccione la función que acaba de crear.

   d. Finalice los pasos restantes para crear la función.

      "Documentos de Google Cloud: Crear una cuenta de servicio"

Resultado

Ahora tiene una cuenta de servicio que puede asignar a la instancia de Connector VM.

Paso 6: Habilita las API de Google Cloud

Se necesitan varias API para poner en marcha Cloud Volumes ONTAP en Google Cloud.

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)
    - API del servicio de gestión de claves de cloud (KMS)

      (Solo es obligatorio si piensas utilizar el backup y la recuperación de datos de BlueXP con claves de cifrado gestionadas por el cliente (CMEK))

Despliegue el conector en modo privado

Pon en marcha el conector en modo privado para poder utilizar BlueXP sin conectividad saliente a la capa de BlueXP SaaS. Para comenzar, instala el Connector, configura BlueXP accediendo a la interfaz de usuario que se ejecuta en el Connector y, a continuación, proporciona los permisos de nube que hayas configurado previamente.

Paso 1: Instale el conector

Descargue el instalador del producto desde el sitio de soporte de NetApp y, a continuación, instale manualmente el conector en su propio host Linux.

Si desea utilizar BlueXP en "Cloud secreto de AWS" o la "Cloud secreto principal de AWS", entonces debe seguir instrucciones separadas para comenzar en esos entornos. "Descubra cómo empezar a utilizar Cloud Volumes ONTAP en el cloud secreto de AWS o en el cloud secreto superior"

Antes de empezar

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"

   Asegúrese de descargar el instalador fuera de línea para redes privadas sin acceso a Internet.

3. Copie el instalador en el host Linux.
4. Asigne permisos para ejecutar el script.

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

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

5. Ejecute el script de instalación:

```
sudo /path/BlueXP-Connector-offline-<version>
```

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

Resultado

El software del conector está instalado. Ya puede configurar BlueXP.

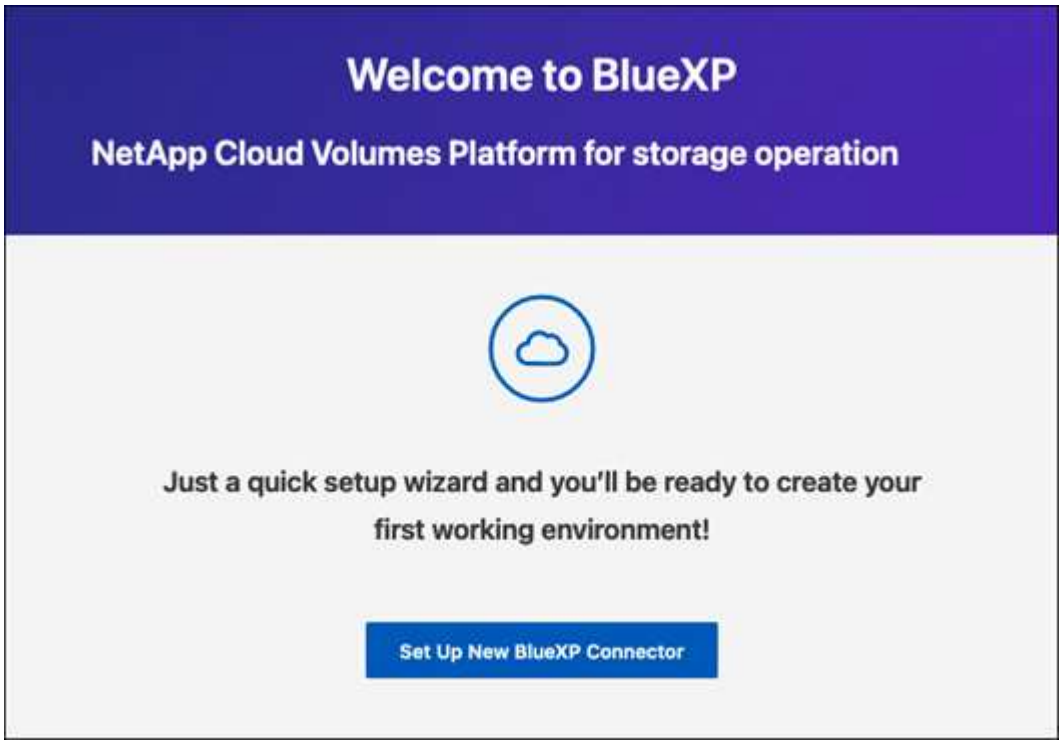
Paso 2: Configura BlueXP

Cuando acceda a la consola BlueXP por primera vez, se le solicitará que configure BlueXP.

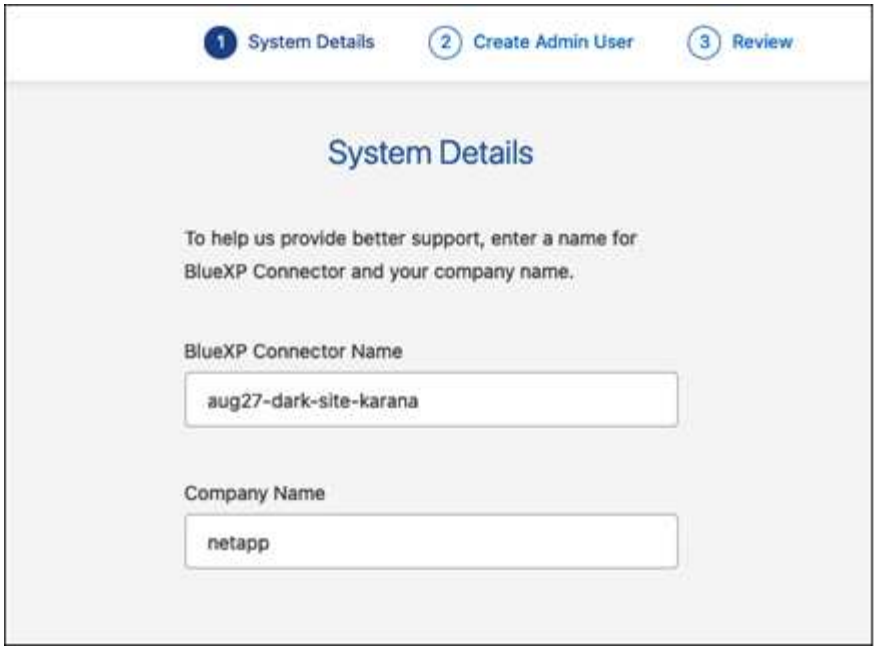
Pasos

1. Abra un explorador web e introduzca https://ipaddress Donde ipaddress es la dirección IP del host Linux en el que instaló el conector.

   Debe ver la siguiente pantalla.



2. Selecciona **Configurar nuevo conector BlueXP** y sigue las indicaciones para configurar el sistema.
   - **Detalles del sistema**: Introduzca un nombre para el conector y el nombre de su empresa.



- **Crear un usuario administrador**: Crea 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**: Revisa los detalles, acepta el contrato de licencia y luego selecciona **Configurar**.

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

Resultado

El conector ahora está instalado y configurado.

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

El futuro

Proporcione a BlueXP los permisos que configuró anteriormente.

Paso 3: Proporcionar permisos a BlueXP

Si desea crear entornos de trabajo de Cloud Volumes ONTAP, tendrá que proporcionar a BlueXP los permisos de cloud que configuró anteriormente.

"Aprenda cómo preparar los permisos en el cloud".

Rol IAM de AWS

Conecte la función IAM que ha creado previamente a la instancia de Connector EC2.

Pasos

1. Vaya a la consola de Amazon EC2.
2. Seleccione **instancias**.
3. Seleccione la instancia de conector.
4. Seleccione **acciones > Seguridad > Modificar función IAM**.
5. Seleccione el rol de IAM y seleccione **Actualizar rol de IAM**.

Resultado

BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

Clave de acceso de AWS

Proporcione a BlueXP la clave de acceso de AWS para un usuario de IAM que tenga los permisos necesarios.

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Servicios Web de Amazon > conector**.
   b. **Definir credenciales**: Introduzca una clave de acceso y una clave secreta de AWS.
   c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.
   d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

Rol de Azure

Vaya al portal de Azure y asigne el rol personalizado de Azure a la máquina virtual Connector para una o más suscripciones.

Pasos

1. En el Portal de Azure, abra el servicio **Suscripciones** y seleccione su suscripción.

   Es importante asignar el rol desde el servicio **Suscripciones** porque especifica el alcance de la asignación de rol en el nivel de suscripción. El *scope* define el juego de recursos al que se aplica el acceso. Si especifica un ámbito a otro nivel (por ejemplo, a nivel de máquina virtual), se verá afectada su capacidad para completar acciones desde BlueXP.

"Documentación de Microsoft Azure: Conozca el ámbito de control de acceso basado en roles de Azure"

2. Selecciona **Control de acceso (IAM)** > **Añadir** > **Añadir asignación de rol**.
3. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **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.

4. En la ficha **Miembros**, realice los siguientes pasos:
   a. Asignar acceso a una **identidad administrada**.
   b. Seleccione **Seleccionar miembros**, seleccione la suscripción en la que se creó la máquina virtual Connector, en **Identidad administrada**, elija **Máquina virtual** y, a continuación, seleccione la máquina virtual Connector.
   c. Selecciona **Seleccionar**.
   d. Seleccione **Siguiente**.
   e. Seleccione **revisar + asignar**.
   f. Si desea administrar recursos en suscripciones adicionales de Azure, cambie a esa suscripción y repita estos pasos.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Servicio principal de Azure

Proporcione a BlueXP las credenciales para la entidad de servicio de Azure que configuró anteriormente.

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.
   b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:
      - ID de aplicación (cliente)
      - ID de directorio (inquilino)
      - Secreto de cliente
   c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.
   d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Cuenta de servicio de Google Cloud

Asocie la cuenta de servicio a la máquina virtual del conector.

Pasos

1. Vaya al portal de Google Cloud y asigne la cuenta de servicio a la instancia de Connector VM.

   "Documentación de Google Cloud: Cambiar la cuenta de servicio y los ámbitos de acceso para una instancia"

2. Si quieres gestionar recursos en otros proyectos, otorga acceso agregando la cuenta de servicio con el rol BlueXP a ese proyecto. Deberá repetir este paso con cada proyecto.

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Google Cloud en su nombre.

Qué puede hacer después (modo privado)

Después de empezar a utilizar BlueXP en modo privado, puede empezar a utilizar los servicios BlueXP compatibles con modo privado.

Si necesita ayuda, consulte la siguiente documentación:

- "Creación de sistemas Cloud Volumes ONTAP"
- "Detectar clústeres de ONTAP en las instalaciones"
- "Replicar datos"
- "Analiza los datos de volúmenes de ONTAP on-premises con la clasificación de BlueXP"
- "Haz un backup de los datos de volúmenes de ONTAP en las instalaciones en StorageGRID mediante el backup y la recuperación de BlueXP"

Enlace relacionado

"Modos de implementación de BlueXP"

Inicie sesión en BlueXP

La forma en que inicies sesión en BlueXP depende del modo de puesta en marcha de BlueXP que utilices en tu cuenta.

Modo estándar

Después de registrarte en BlueXP, puedes iniciar sesión desde la consola web para empezar a gestionar tu infraestructura de datos y almacenamiento.

Acerca de esta tarea

Puede iniciar sesión en la consola basada en Web de BlueXP mediante 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). "Aprenda a usar la federación de identidades con BlueXP".

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.

Modo restringido

Cuando utilizas BlueXP en modo restringido, tendrás que iniciar sesión en la consola de BlueXP desde la interfaz de usuario que se ejecuta localmente en Connector.

Acerca de esta tarea

BlueXP permite iniciar sesión con una de las siguientes opciones cuando su cuenta está configurada en modo restringido:

- 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). "Aprenda a usar la federación de identidades con BlueXP".

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 en el que instaló el conector. Por ejemplo, es posible que necesite introducir una dirección IP privada de un host que tenga una conexión con el host Connector.

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

Resultado

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

Modo privado

Cuando utiliza BlueXP en modo privado, tendrá que iniciar sesión en la consola de BlueXP desde la interfaz de usuario que se ejecuta localmente en Connector.

Acerca de esta tarea

El modo privado admite la gestión de usuarios locales y el acceso. La autenticación no se proporciona a través del servicio en la nube de BlueXP.

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 en el que instaló el conector. Por ejemplo, es posible que necesite introducir una dirección IP privada de un host que tenga una conexión con el host Connector.

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

Resultado

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

Administrar BlueXP

Uso de la federación de identidades con BlueXP

Identity federation habilita el inicio de sesión único con BlueXP para que los usuarios puedan iniciar sesión utilizando credenciales de su identidad corporativa. Para empezar, aprenda cómo funciona Identity federation con BlueXP y, a continuación, revise una descripción general del proceso de configuración.

federación de identidades con credenciales de NSS

Si utiliza sus credenciales del sitio de soporte de NetApp (NSS) para iniciar sesión en BlueXP, no debe seguir las instrucciones de esta página para configurar la federación de identidades. Debe hacer lo siguiente en su lugar:

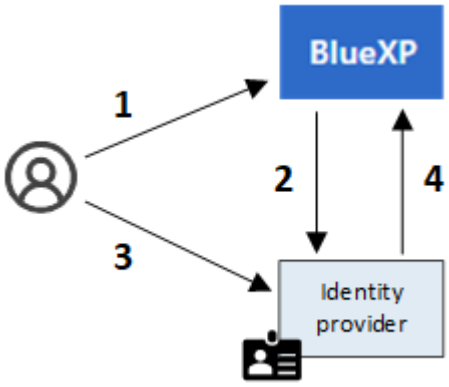
- Descargue y complete el "Formulario de solicitud de federación de NetApp"
- Envíe el formulario a la dirección de correo electrónico especificada en el formulario

El equipo de gestión de acceso e identidad de NetApp revisará su solicitud.

Cómo funciona la federación de identidades

La configuración de la federación de identidades crea una conexión de confianza entre el proveedor de servicios de autenticación (auth0) de BlueXP y su propio proveedor de gestión de identidades.

La siguiente imagen muestra cómo funciona la federación de identidades con BlueXP:



1. Un usuario introduce su dirección de correo electrónico en la página de inicio de sesión de BlueXP.
2. BlueXP identifica que el dominio de correo electrónico forma parte de una conexión federada y envía la solicitud de autenticación al proveedor de identidades mediante la conexión de confianza.

   Al configurar una conexión federada, BlueXP siempre utiliza esa conexión federada para la autenticación.

3. El usuario autentica mediante credenciales de su directorio corporativo.
4. El proveedor de identidades autentica la identidad del usuario y el usuario inicia sesión en BlueXP.

La federación de identidades usa estándares abiertos, como el lenguaje de marcado de aserción de seguridad 2.0 (SAML) y OpenID Connect (OIDC).

Proveedores de identidades compatibles

BlueXP admite los siguientes proveedores de identidades:

- Proveedores de identidad del lenguaje de marcado de aserción de seguridad (SAML)
- ID de Microsoft Entra
- Servicios de Federación de Active Directory (ADFS).
- PingFederate

BlueXP admite únicamente SSO iniciado por el proveedor de servicios (iniciado por el SP). No se admite el inicio de sesión único iniciado por el proveedor de identidades (IDP).

Descripción general del proceso de configuración

Antes de configurar una conexión entre BlueXP y su proveedor de gestión de identidades, debe comprender los pasos que debe seguir para que pueda prepararse en consecuencia.

Estos pasos son específicos para los usuarios que inician sesión en BlueXP mediante un inicio de sesión en la nube de NetApp. Si utilizas tus credenciales de NSS para iniciar sesión en BlueXP, Aprenda a configurar la federación de identidades con las credenciales de NSS.

Proveedor de identidades SAML

En un nivel superior, la configuración de una conexión federada entre BlueXP y un proveedor de identidades SAML incluye los siguientes pasos:

Paso	Completado por	Descripción
1	Administrador de Active Directory (AD)	Configure su proveedor de identidades SAML para habilitar la federación de identidades con BlueXP. Vea instrucciones para el proveedor de identidades SAML: • "ADFS" • "De acuerdo" • "Inicio de sesión OneLogin" • "PingFederate" • "Salesforce" • "SiteMinder" • "SSOCircle" Si su proveedor de identidades no aparece en la lista anterior, "siga estas instrucciones genéricas" Do *not* complete los pasos que describen cómo crear una conexión en auth0. Creará esa conexión en el siguiente paso.

Paso	Completado por	Descripción
2	Administrador de BlueXP	Vaya a la "Página NetApp Federation Setup" Y cree la conexión con BlueXP. Para completar este paso, debe obtener lo siguiente del administrador de AD acerca del proveedor de identidades: • URL de inicio de sesión • Un certificado de firma X509 (formato PEM o CER) • URL de cierre de sesión (opcional) Después de crear la conexión mediante esta información, la página Federation Setup (Configuración de Federación) enumera los parámetros que puede enviar al administrador de AD para completar la configuración en el paso siguiente. Tome nota de la fecha de vencimiento del certificado. Debe volver a la página de configuración de federación y actualizar el certificado *before* que caduque. Esta es tu responsabilidad. BlueXP no realiza un seguimiento de la fecha de caducidad. Es mejor trabajar con su equipo de AD para recibir alertas a tiempo.
3	Administrador DE ANUNCIOS	Complete la configuración en el proveedor de identidades utilizando los parámetros que se muestran en la página Federation Setup (Configuración de Federación) después de finalizar el paso 2.
4	Administrador de BlueXP	Compruebe y active la conexión desde "Página NetApp Federation Setup" Tenga en cuenta que la página se actualiza entre probar la conexión y habilitar la conexión.

ID de Microsoft Entra

En un nivel general, la configuración de una conexión federada entre BlueXP y Microsoft Entra ID incluye los siguientes pasos:

Paso	Completado por	Descripción
1	Administrador DE ANUNCIOS	Configura Microsoft Entra ID para habilitar la federación de identidades con BlueXP. "Vea las instrucciones para registrar la aplicación con Microsoft Entra ID" Do *not* complete los pasos que describen cómo crear una conexión en auth0. Creará esa conexión en el siguiente paso.

Paso	Completado por	Descripción
2	Administrador de BlueXP	Vaya a la "Página NetApp Federation Setup" Y cree la conexión con BlueXP. Para completar este paso, debe obtener lo siguiente de su administrador de AD: • ID del cliente • Valor secreto cliente • Dominio de Microsoft Entra ID Después de crear la conexión mediante esta información, la página Federation Setup (Configuración de Federación) enumera los parámetros que puede enviar al administrador de AD para completar la configuración en el paso siguiente. Tome nota de la fecha de caducidad de la clave secreta. Debe volver a la página de configuración de federación y actualizar el certificado *before* que caduque. Esta es tu responsabilidad. BlueXP no realiza un seguimiento de la fecha de caducidad. Es mejor trabajar con su equipo de AD para recibir alertas a tiempo.
3	Administrador DE ANUNCIOS	Complete la configuración en Microsoft Entra ID utilizando los parámetros que se muestran en la página Configuración de federación después de finalizar el paso 2.
4	Administrador de BlueXP	Compruebe y active la conexión desde "Página NetApp Federation Setup" Tenga en cuenta que la página se actualiza entre probar la conexión y habilitar la conexión.

ADFS

En un nivel alto, la configuración de una conexión federada entre BlueXP y ADFS incluye los siguientes pasos:

Paso	Completado por	Descripción
1	Administrador DE ANUNCIOS	Configure el servidor ADFS para habilitar la federación de identidades con BlueXP. "Vea las instrucciones para configurar el servidor ADFS con auth0"

Paso	Completado por	Descripción
2	Administrador de BlueXP	Vaya a la "Página NetApp Federation Setup" Y cree la conexión con BlueXP. Para completar este paso, debe obtener lo siguiente del administrador de AD: La dirección URL del servidor ADFS o del archivo de metadatos de federación. Después de crear la conexión mediante esta información, la página Federation Setup (Configuración de Federación) enumera los parámetros que puede enviar al administrador de AD para completar la configuración en el paso siguiente. Tome nota de la fecha de vencimiento del certificado. Debe volver a la página de configuración de federación y actualizar el certificado *before* que caduque. Esta es tu responsabilidad. BlueXP no realiza un seguimiento de la fecha de caducidad. Es mejor trabajar con su equipo de AD para recibir alertas a tiempo.
3	Administrador DE ANUNCIOS	Complete la configuración en el servidor ADFS utilizando los parámetros que se muestran en la página Federation Setup después de finalizar el paso 2.
4	Administrador de BlueXP	Compruebe y active la conexión desde "Página NetApp Federation Setup" Tenga en cuenta que la página se actualiza entre probar la conexión y habilitar la conexión.

PingFederate

En un nivel alto, la configuración de una conexión federada entre BlueXP y un servidor PingFederate incluye los siguientes pasos:

Paso	Completado por	Descripción
1	Administrador DE ANUNCIOS	Configure su servidor PingFederate para habilitar la federación de identidades con BlueXP. "Vea las instrucciones para crear una conexión" Do *not* complete los pasos que describen cómo crear una conexión en auth0. Creará esa conexión en el siguiente paso.

Paso	Completado por	Descripción
2	Administrador de BlueXP	Vaya a la "Página NetApp Federation Setup" Y cree la conexión con BlueXP. Para completar este paso, debe obtener lo siguiente de su administrador de AD: • La URL del servidor PingFederate • Un certificado de firma X509 (formato PEM o CER) Después de crear la conexión mediante esta información, la página Federation Setup (Configuración de Federación) enumera los parámetros que puede enviar al administrador de AD para completar la configuración en el paso siguiente. Tome nota de la fecha de vencimiento del certificado. Debe volver a la página de configuración de federación y actualizar el certificado *before* que caduque. Esta es tu responsabilidad. BlueXP no realiza un seguimiento de la fecha de caducidad. Es mejor trabajar con su equipo de AD para recibir alertas a tiempo.
3	Administrador DE ANUNCIOS	Complete la configuración en el servidor PingFederate utilizando los parámetros que se muestran en la página Federation Setup después de finalizar el paso 2.
4	Administrador de BlueXP	Compruebe y active la conexión desde "Página NetApp Federation Setup" Tenga en cuenta que la página se actualiza entre probar la conexión y habilitar la conexión.

Actualización de una conexión federada

Una vez que el administrador de BlueXP activa una conexión, el administrador puede actualizar la conexión en cualquier momento desde la "Página NetApp Federation Setup"

Por ejemplo, es posible que deba actualizar la conexión cargando un nuevo certificado.

El administrador de BlueXP que creó la conexión es el único usuario autorizado que puede actualizar la conexión. Si desea añadir más administradores, póngase en contacto con el servicio de soporte de NetApp.

Cuentas BlueXP

Administre su cuenta de BlueXP

Cuando creas una cuenta de BlueXP, solo incluye un solo usuario administrador y un espacio de trabajo. Puede administrar la cuenta para que se adapte a las necesidades de su organización agregando usuarios, creando cuentas de servicio con fines de automatización, agregando espacios de trabajo, etc.

"Descubre cómo funcionan las cuentas de BlueXP".

Gestione su 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 los recursos y gestionarlos en espacios de trabajo específicos.

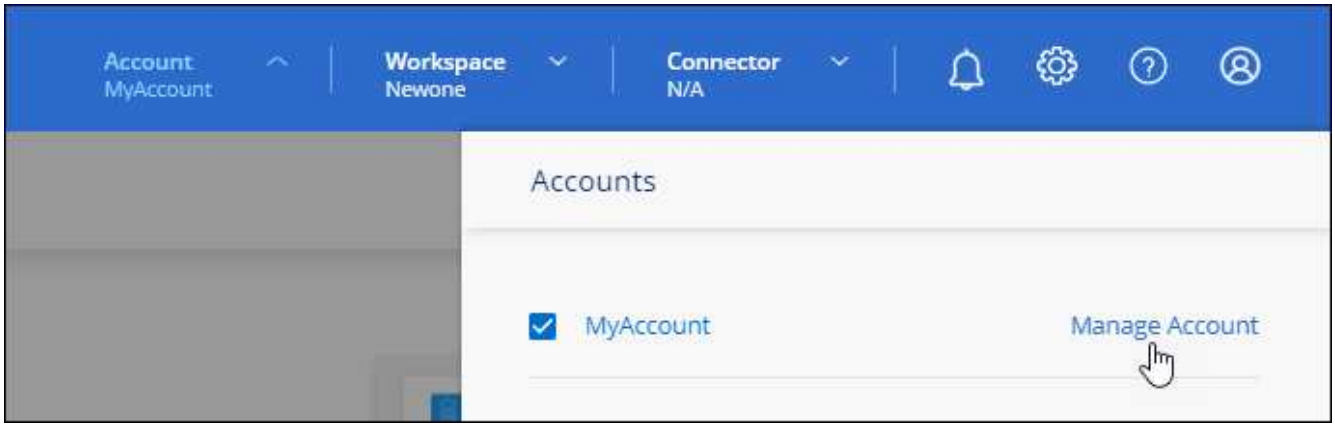
Añadir usuarios

Asocie usuarios a su cuenta de BlueXP para que esos usuarios puedan crear y administrar entornos de trabajo en BlueXP.

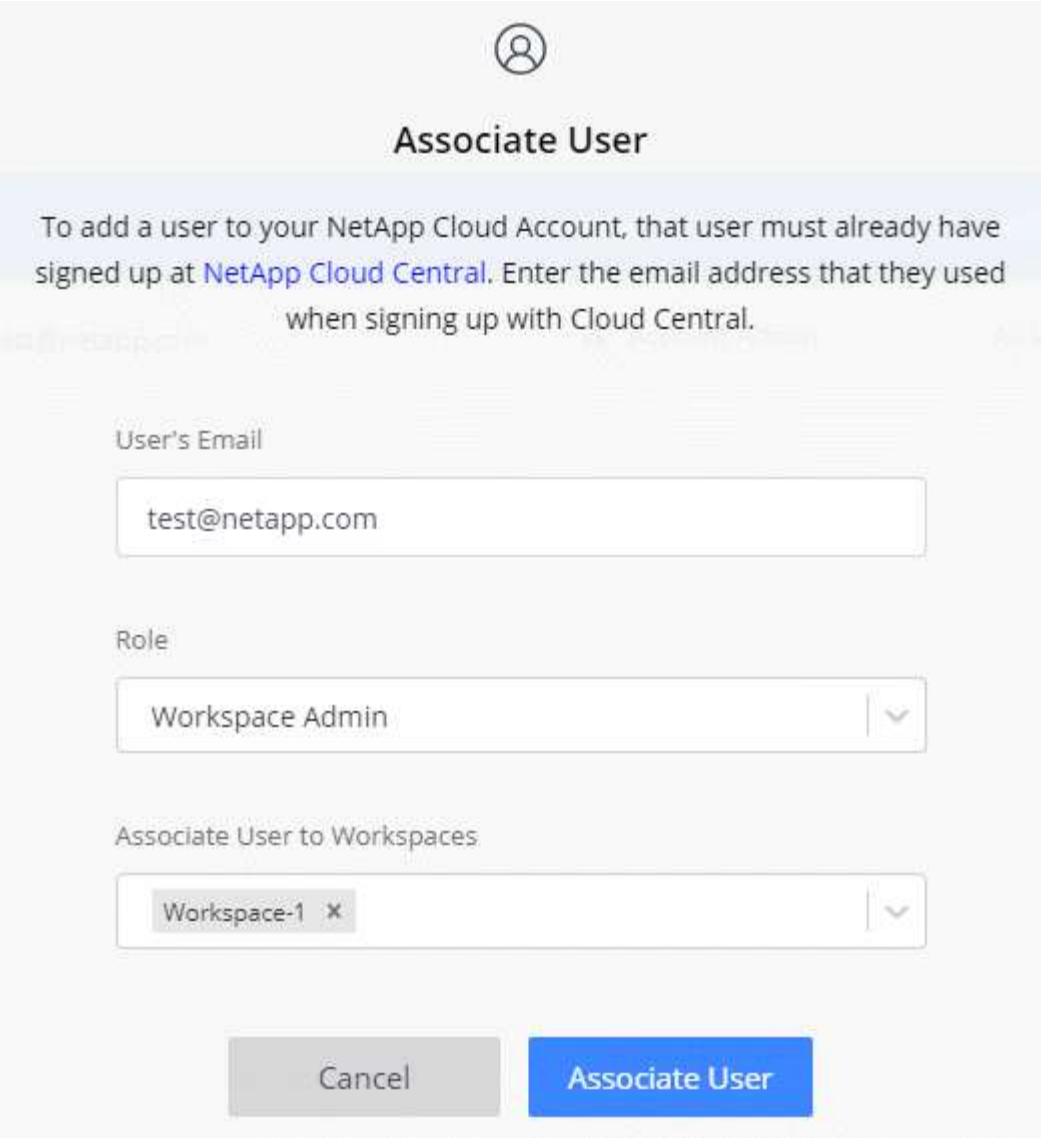
Pasos

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, seleccione la lista desplegable **cuenta**.

3. Seleccione **Administrar cuenta** junto a la cuenta seleccionada actualmente.



4. En la ficha Miembros, seleccione **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**: Solo puede ver la información de cumplimiento para la clasificación de BlueXP y generar informes para espacios de trabajo a los que tienen permiso para acceder.
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.



7. Seleccione **asociado**.

Resultado

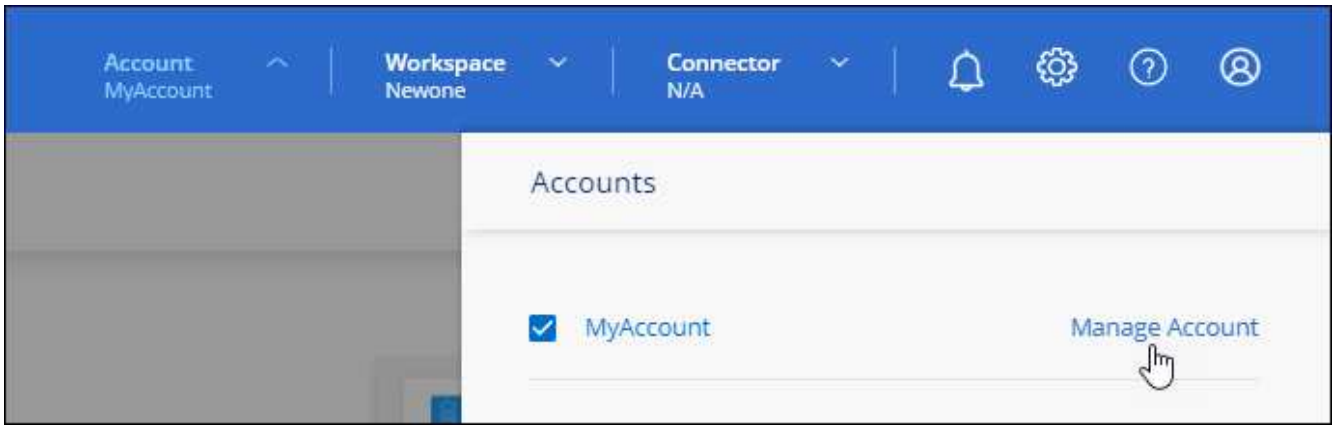
El usuario debe recibir un correo electrónico de NetApp BlueXP titulado "Account Association". El correo electrónico incluye la información necesaria para acceder a BlueXP.

Quitar usuarios

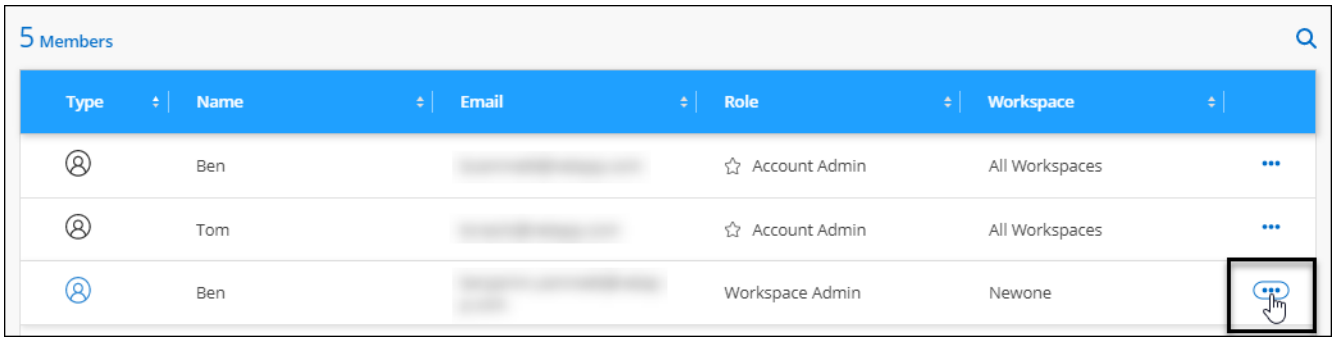
Al desasociar un usuario, ya no pueden acceder a los recursos de una cuenta de BlueXP.

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.



2. En la ficha Miembros, seleccione el menú de acciones de la fila correspondiente al usuario.



3. Seleccione **desasociar usuario** y seleccione **desasociar** para confirmar.

Resultado

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

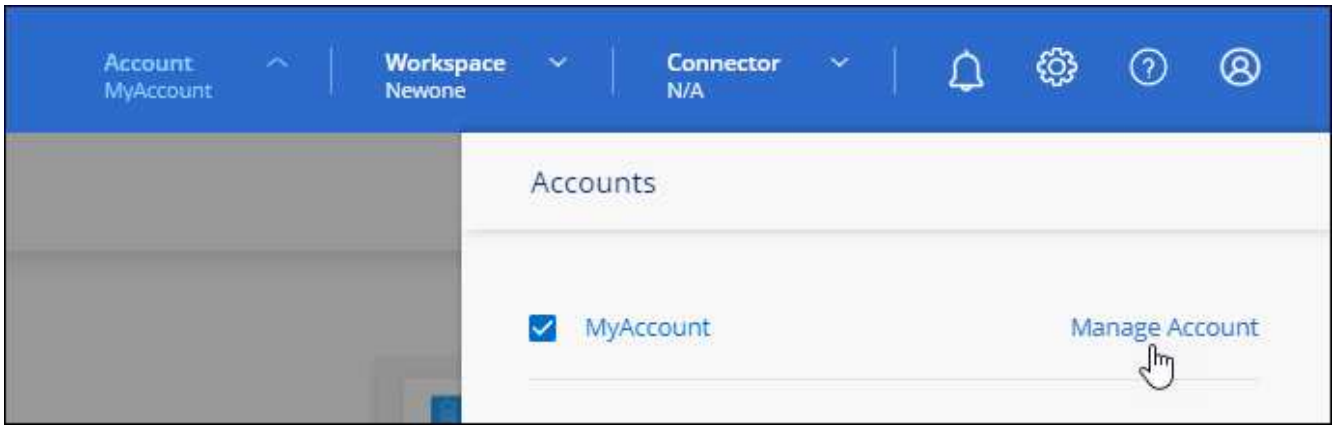
Administrar los espacios de trabajo de un administrador de área de trabajo

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.

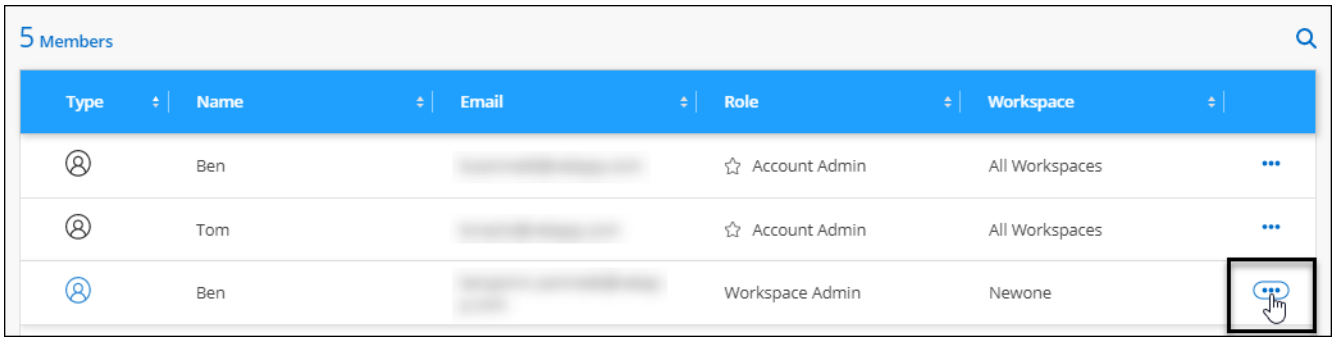
> También debes asociar el conector a los espacios de trabajo para que los administradores de espacios de trabajo puedan acceder a esos espacios de trabajo desde BlueXP. "Aprenda a administrar los espacios de trabajo de Connector".

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.



2. En la ficha Miembros, seleccione el menú de acciones de la fila correspondiente al usuario.



3. Seleccione **gestionar espacios de trabajo**.
4. Seleccione los espacios de trabajo que desea asociar con el usuario y seleccione **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.

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.

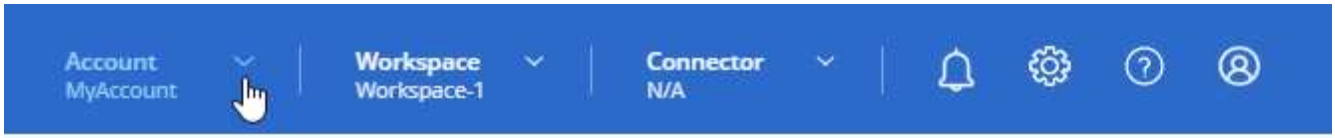
Tenga en cuenta que un token de actualización no es necesario para las operaciones de API cuando se utiliza una cuenta de servicio. "Obtenga más información sobre los tokens de actualización"

Cree una cuenta de servicio

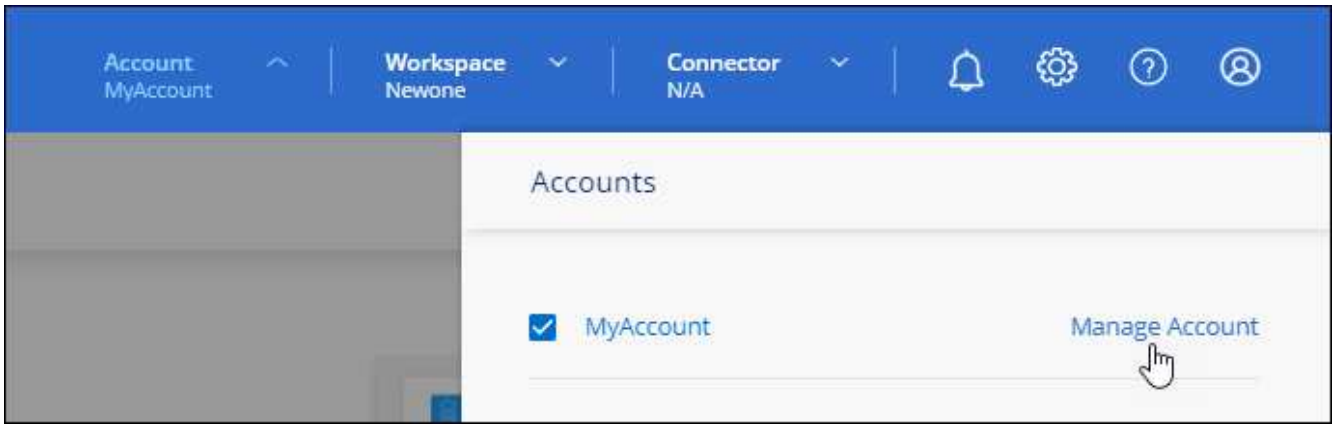
Cree tantas cuentas de servicio como necesite para gestionar los recursos en sus entornos de trabajo.

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta**.



2. Seleccione **Administrar cuenta** junto a la cuenta seleccionada actualmente.



3. En la ficha Miembros, seleccione **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. Seleccione **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. Seleccione **Cerrar**.

Obtener 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.

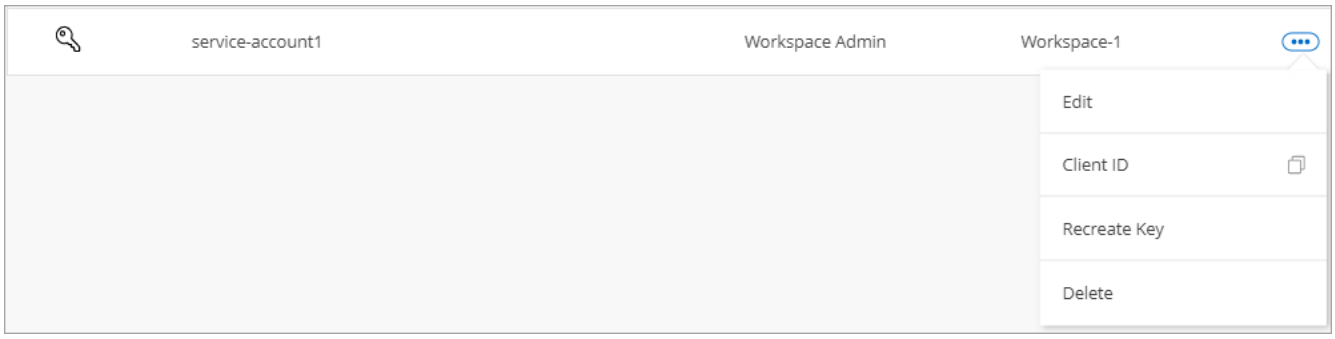
"Aprenda a crear un token de cuenta de servicio"

Copie el ID del cliente

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

Pasos

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



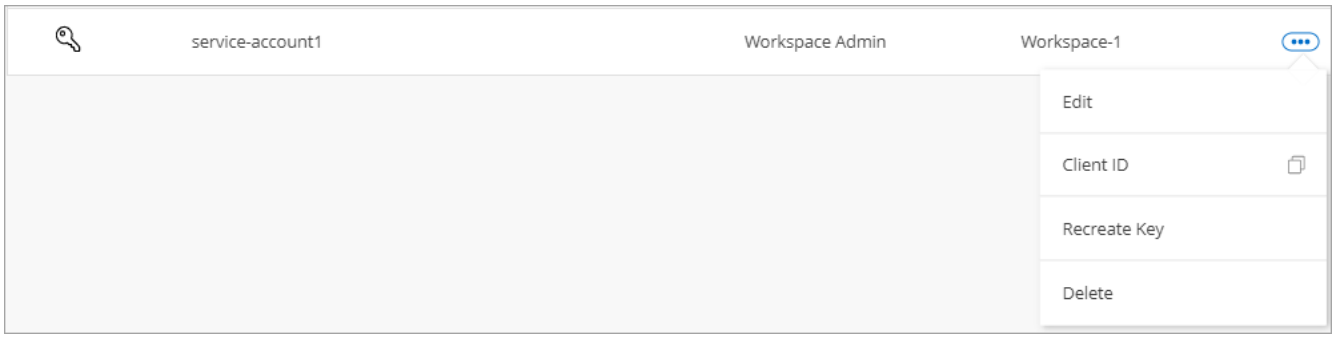
2. Seleccione **ID de cliente**.
3. El ID se copia en el portapapeles.

Vuelva a crear las 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 tecla anterior.

Pasos

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



2. Seleccione **Volver a crear clave**.
3. Seleccione **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.

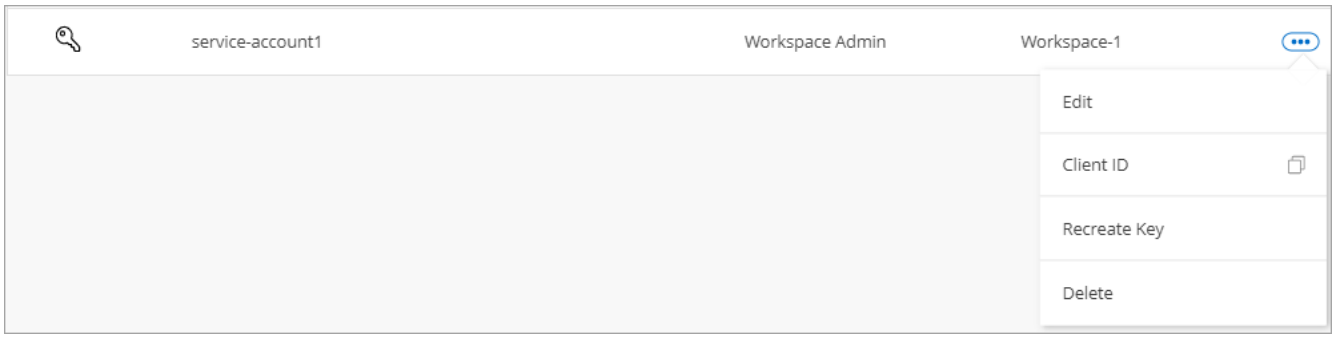
5. Seleccione **Cerrar**.

Eliminar una cuenta de servicio

Elimine una cuenta de servicio si ya no necesita utilizarla.

Pasos

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



2. Seleccione **Eliminar**.
3. Seleccione **Eliminar** de nuevo para confirmar.

Administrar 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, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.
2. Seleccione **espacios de trabajo**.
3. Seleccione una de las siguientes opciones:
   - Seleccione **Agregar nuevo espacio de trabajo** para crear un nuevo espacio de trabajo.
   - Seleccione **Cambiar nombre** para cambiar el nombre del espacio de trabajo.
   - Seleccione **Eliminar** para eliminar el espacio de trabajo.

   Si ha creado un nuevo espacio de trabajo, también debe agregar Connector a ese espacio de trabajo. Si no agrega Connector, los administradores de Workspace no podrán acceder a ninguno de los recursos del espacio de trabajo. Consulte la siguiente sección para obtener más detalles.

Administrar 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, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.
2. Seleccione **conector**.
3. Seleccione **Administrar espacios de trabajo** para el conector que desea asociar.
4. Seleccione las áreas de trabajo que desea asociar con el conector y seleccione **aplicar**.

Cambie el nombre de su cuenta

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

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.
2. En la ficha **Descripción general**, seleccione el icono de edición junto al nombre de la cuenta.
3. Escriba un nuevo nombre de cuenta y seleccione **Guardar**.

Permitir vistas previas privadas

Permita que las vistas previas privadas de su cuenta tengan acceso a nuevos servicios 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, seleccione la lista desplegable **cuenta** y seleccione **gestionar 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, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.
2. En la ficha **Descripción general**, active la opción **permitir servicios de terceros**.

Supervisar las 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.

En la siguiente tabla se ofrece una comparación entre el Centro de notificaciones y la línea de tiempo para que pueda entender lo que cada uno puede ofrecer.

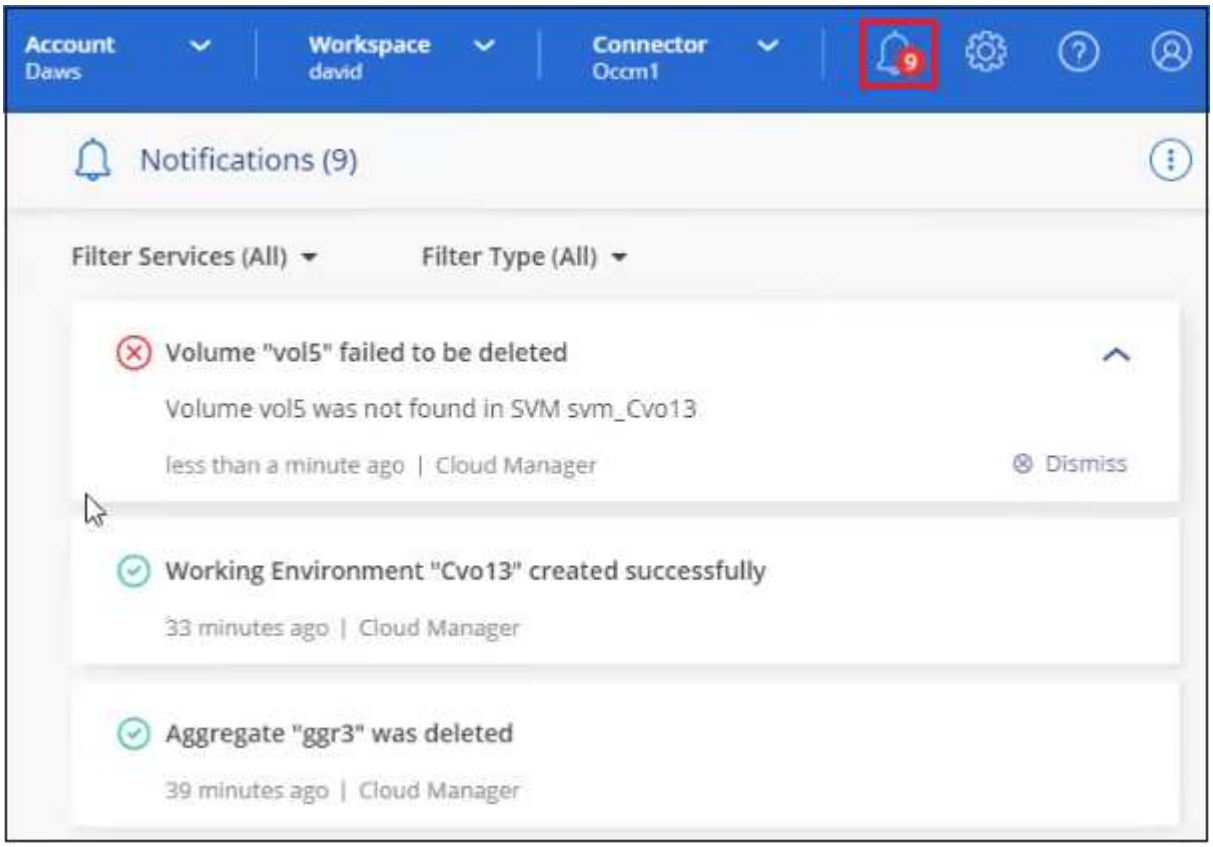
Centro de notificaciones	Línea de tiempo
Muestra el estado de alto nivel de eventos y acciones	Proporciona detalles sobre cada evento o acción para una investigación posterior
Muestra el estado de la sesión de inicio de sesión actual (la información no aparecerá en el Centro de notificaciones después 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

Centro de notificaciones	Línea de tiempo
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

Supervise las actividades mediante el Centro de notificaciones

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 de BlueXP informan información en el Centro de notificaciones en este momento.

Puede visualizar las notificaciones seleccionando 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 ciertos tipos de notificaciones por correo electrónico de modo que se le informe de la actividad importante del sistema incluso cuando no haya iniciado sesión en el sistema. Los correos electrónicos se pueden enviar a cualquier usuario que forme parte de su cuenta de BlueXP o a cualquier otro destinatario que necesite conocer ciertos tipos de actividad del sistema. Descubra cómo defina los ajustes de notificación por correo electrónico.

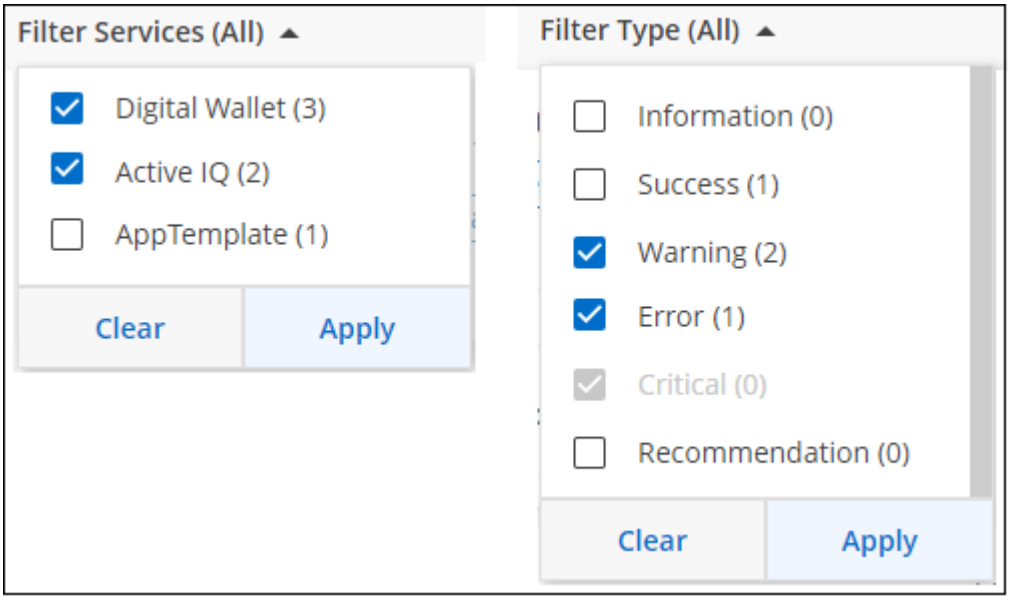
Tipos de notificación

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.

Filtrar notificaciones

De forma predeterminada, verá todas las notificaciones activas en el Centro de notificaciones. Puede filtrar las notificaciones que ve para mostrar solo las notificaciones que son importantes para usted. Puede filtrar por "Servicio" de BlueXP y por "Tipo" de notificación.



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.

Descartar notificaciones

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, seleccione ⋮ Y selecciona **descartar todo**.

Para descartar notificaciones individuales, coloque el cursor sobre la notificación y seleccione **descartar**.

Establecer 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 se pueden enviar a cualquier usuario que forme parte de su cuenta de BlueXP o a cualquier otro destinatario que necesite conocer ciertos tipos de actividad del sistema.

- En este momento, se envían notificaciones por correo electrónico para obtener las siguientes funciones y servicios de BlueXP: Conector, cartera digital de BlueXP, copia y sincronización de BlueXP, backup y recuperación de BlueXP, organización en niveles de BlueXP e informes de migración de BlueXP. 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.

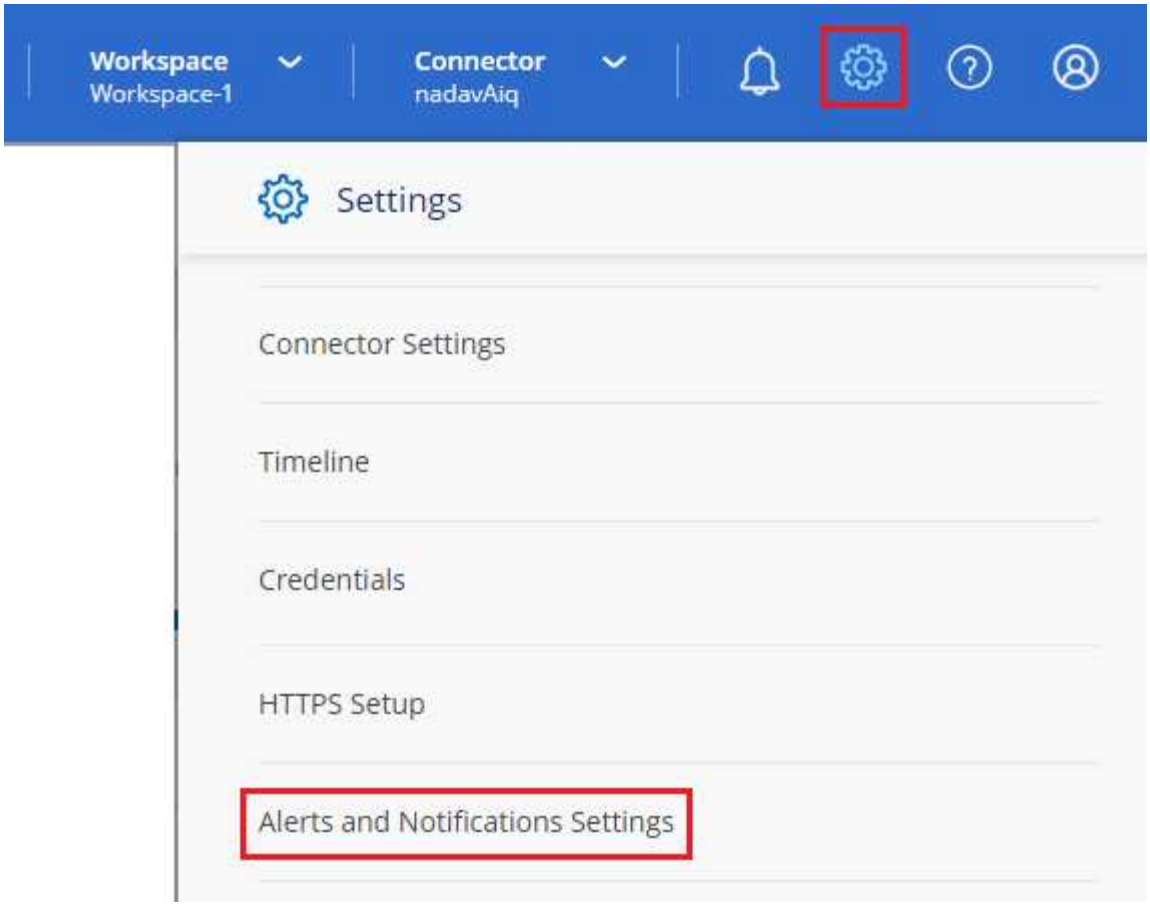
Los filtros que establezca en el Centro de notificaciones no determinan los tipos de notificaciones que recibirá por correo electrónico. De forma predeterminada, los administradores de cuentas de BlueXP recibirán correos electrónicos para todas las notificaciones "críticas" y "recomendaciones". Estas notificaciones se realizan en todos los servicios; no puedes elegir recibir notificaciones solo para determinados servicios, como Connectors o la copia de seguridad y recuperación de BlueXP.

Todos los demás usuarios y destinatarios están configurados para no recibir ningún correo electrónico de notificación, por lo que tendrá que configurar la configuración de notificaciones para cualquier usuario adicional.

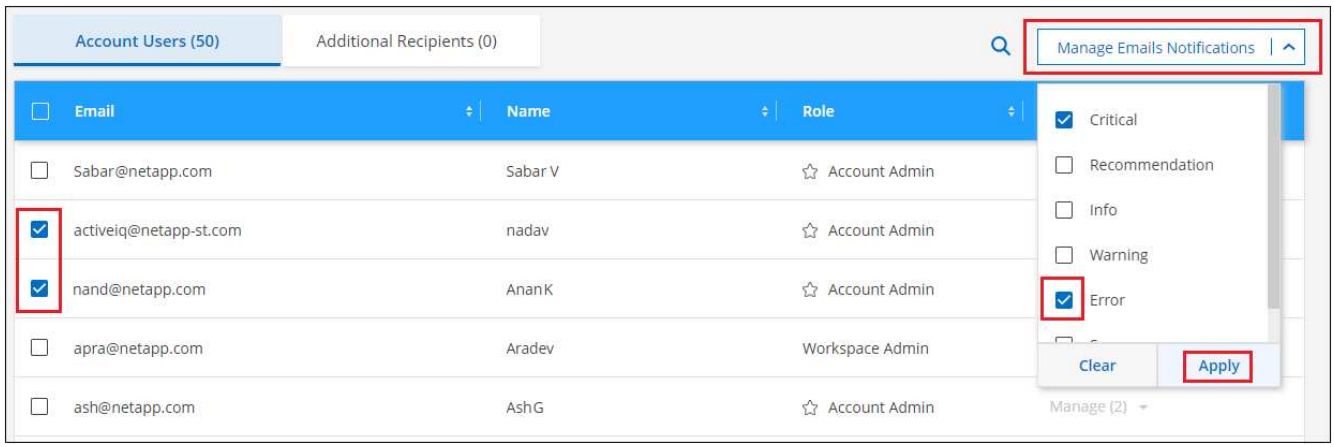
Debe ser un administrador de cuentas para personalizar los ajustes de notificaciones.

Pasos

1. En la barra de menús de BlueXP, seleccione **Configuración > Alertas y Configuración de 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, seleccione el menú en la columna Notificaciones de ese usuario, compruebe los tipos de notificaciones que se van a enviar y seleccione **aplicar**.
    - Para realizar cambios en varios usuarios, marque la casilla de cada usuario, seleccione **Administrar notificaciones por correo electrónico**, seleccione los tipos de notificaciones que desea enviar y seleccione **aplicar**.



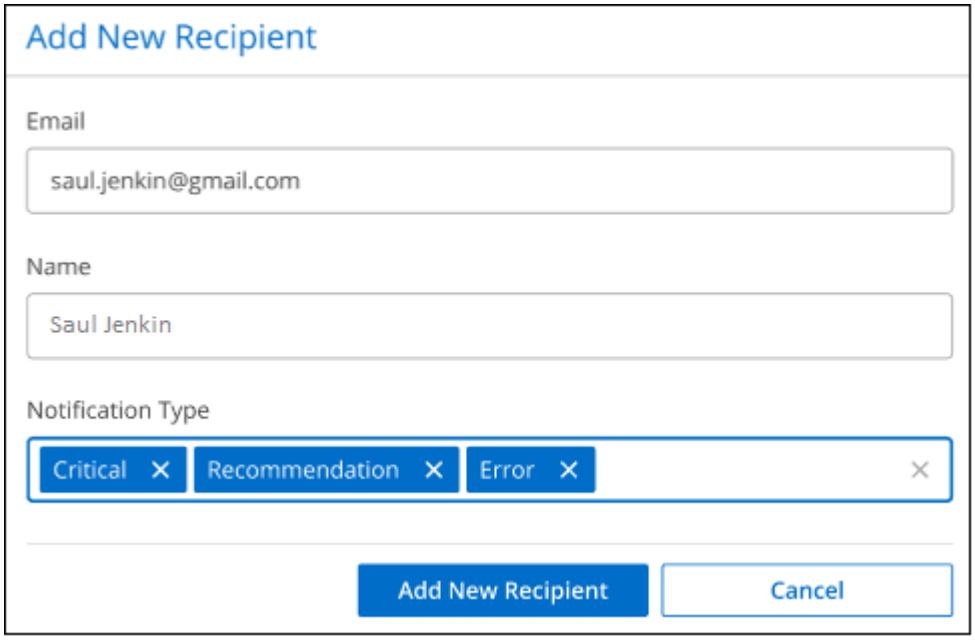
Añada otros destinatarios de correo electrónico

Los usuarios que aparecen en la ficha *Account Users* se rellenan automáticamente desde los usuarios de su cuenta de BlueXP (desde 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, seleccione **Agregar nuevos destinatarios**.



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

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, seleccione **Configuración > línea de tiempo**.
2. En los filtros, seleccione **Servicio**, active **Cliente** y seleccione **aplicar**.

Resultado

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

Cree otra cuenta de BlueXP

Cuando se registra en BlueXP, se le pide que cree una cuenta para su organización. Esta cuenta puede ser todo lo que necesite, pero si su negocio requiere varias cuentas, tendrá que crear cuentas adicionales con la API de tenancy.

Utilice la siguiente llamada a la API para crear una cuenta de BlueXP adicional:

PUBLICAR `/tenancy/account/{accountName}`

Si desea habilitar el modo restringido, debe incluir lo siguiente en el cuerpo de la solicitud:

```
{
  "isSaasDisabled": true
}
```

No se puede cambiar la configuración del modo restringido después de que BlueXP cree la cuenta. No se puede activar el modo restringido más adelante y no se puede desactivar más adelante. Se debe establecer en el momento de crear la cuenta.

"Aprenda a usar esta llamada API"

Enlaces relacionados

- "Obtenga más información sobre las cuentas de BlueXP"
- "Obtenga más información sobre los modos de implementación de BlueXP"

Roles de usuario

Las funciones Administrador de cuentas, Administrador de área de trabajo, Visor de cumplimiento y Administrador de SnapCenter proporcionan permisos específicos a los usuarios. Puedes asignar uno de estos roles cuando asocias un nuevo usuario a tu cuenta de BlueXP.

El rol de Visor de cumplimiento de normativas es para acceso de clasificación de BlueXP de solo lectura.

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
Eliminar entornos de trabajo de un espacio de trabajo	Sí	Sí	No	No
Eliminar 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

Tarea	Administrador de cuentas	Administrador de área de trabajo	Visor de cumplimiento de normativas	Administrador de SnapCenter
Consulta los resultados del análisis de clasificación de BlueXP	Sí	Sí	Sí	No
Reciba el informe de Cloud Volumes ONTAP	Sí	No	No	No
Crear conectores	Sí	No	No	No
Administrar cuentas de BlueXP	Sí	No	No	No
Gestionar credenciales	Sí	No	No	No
Modificar la configuración de BlueXP	Sí	No	No	No
Consulte y gestione la consola de soporte	Sí	No	No	No
Instale un certificado HTTPS	Sí	No	No	No

Enlaces relacionados

- "Configuración de áreas de trabajo y usuarios en la cuenta de BlueXP"
- "Gestión de áreas de trabajo y usuarios en la cuenta de BlueXP"

Conectores

Busque el ID del sistema de un conector

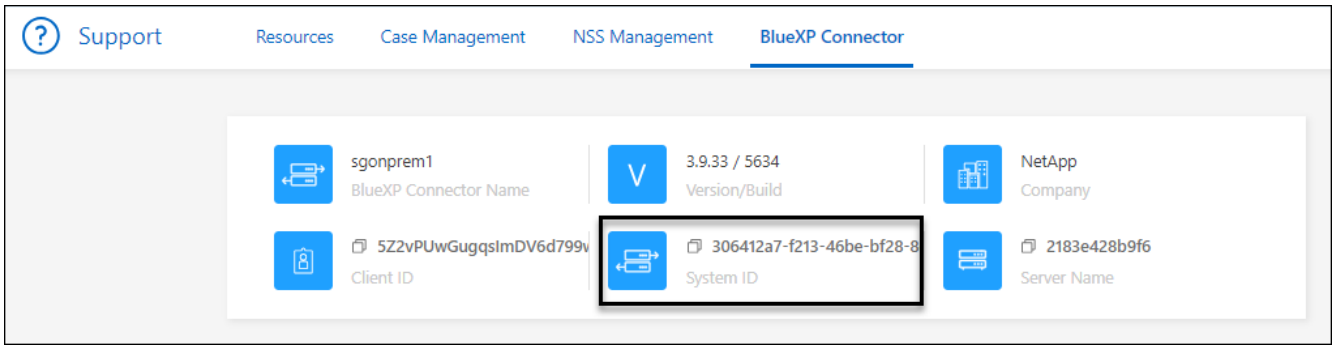
Para ayudarle a comenzar, su representante de NetApp puede pedirle el ID de sistema de su conector. El ID se utiliza normalmente para licencias y solución de problemas.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda.
2. Selecciona **Support > BlueXP Connector**.

   El ID del sistema aparece en la parte superior de la página.

   ejemplo



Administrar conectores existentes

Después de crear un conector, es posible que deba gestionarlo de vez en cuando. Por ejemplo, puede que desee cambiar entre conectores si tiene más de uno. También es posible que debas actualizar manualmente el conector cuando usas BlueXP en modo privado.

"Descubra cómo funcionan los conectores".

> El conector incluye una interfaz de usuario local, a la que se puede acceder desde el host del conector. Esta interfaz de usuario se proporciona a los clientes que utilizan BlueXP en el modo restringido o en el modo privado. Cuando utiliza BlueXP en el modo estándar, debe acceder a la interfaz de usuario desde "Consola de SaaS de BlueXP"
>
> "Obtenga más información sobre los modos de implementación de BlueXP".

Mantenimiento del sistema operativo y los equipos virtuales

El mantenimiento del sistema operativo en el host del conector es responsabilidad suya. Por ejemplo, debe aplicar actualizaciones de seguridad al sistema operativo en el host del conector siguiendo los procedimientos estándar de su empresa para la distribución del sistema operativo.

Tenga en cuenta que no es necesario detener ningún servicio en el host del conector cuando se ejecuta una actualización del SO.

Si necesita parar e iniciar el conector VM, debe hacerlo desde la consola de su proveedor de cloud o mediante los procedimientos estándar para la gestión en las instalaciones.

"Tenga en cuenta que el conector debe estar operativo en todo momento".

Tipo de máquina virtual o instancia

Si creaste un Connector directamente desde BlueXP, BlueXP implementó una instancia de máquina virtual en tu proveedor de nube con una configuración predeterminada. Después de crear el conector, no debe cambiar a una instancia de VM más pequeña que tenga menos CPU o RAM.

Los requisitos de CPU y RAM son los siguientes:

CPU

4 núcleos o 4 vCPU

RAM

14 GB

"Obtenga información sobre la configuración predeterminada para el conector".

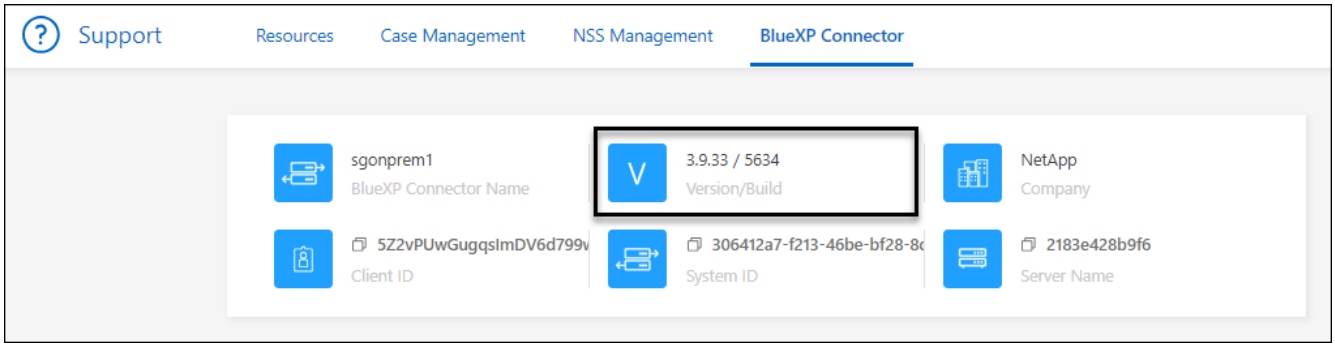
Ver la versión de un conector

Puede ver la versión de su conector para verificar que el conector se actualiza automáticamente a la última versión o porque necesita compartirlo con su representante de NetApp.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda.
2. Selecciona **Support > BlueXP Connector**.

   La versión se muestra en la parte superior de la página.



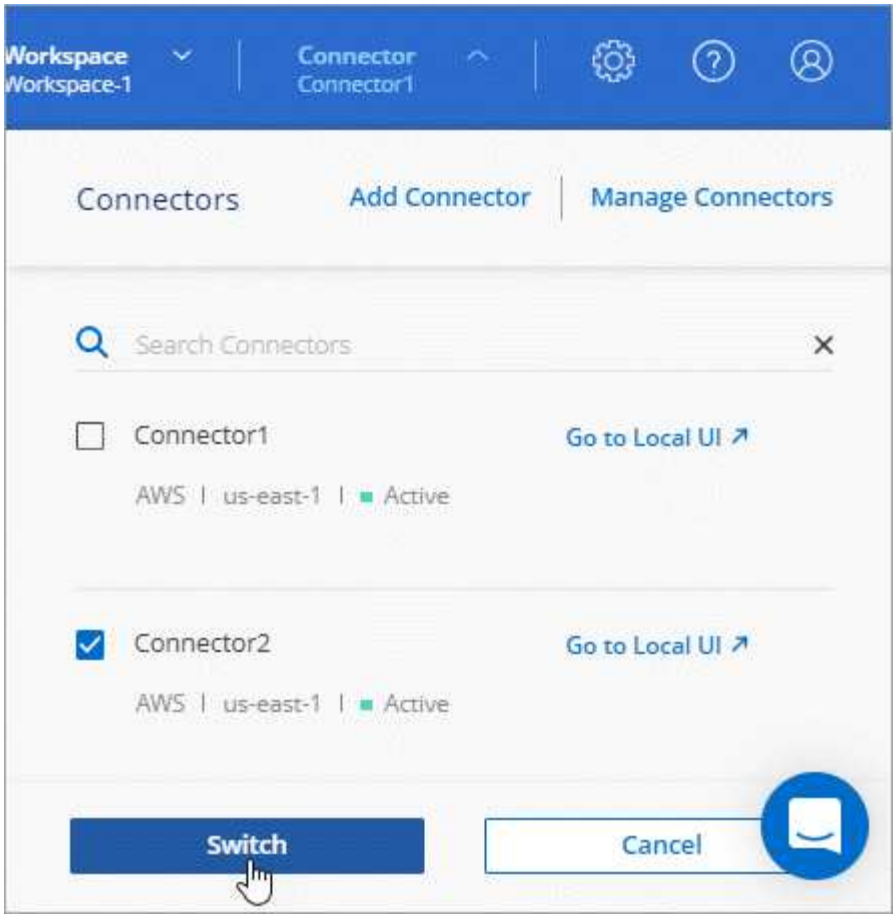
Cambiar entre conectores

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. Seleccione la lista desplegable **conector**, seleccione otro conector y, a continuación, seleccione **interruptor**.



Resultado

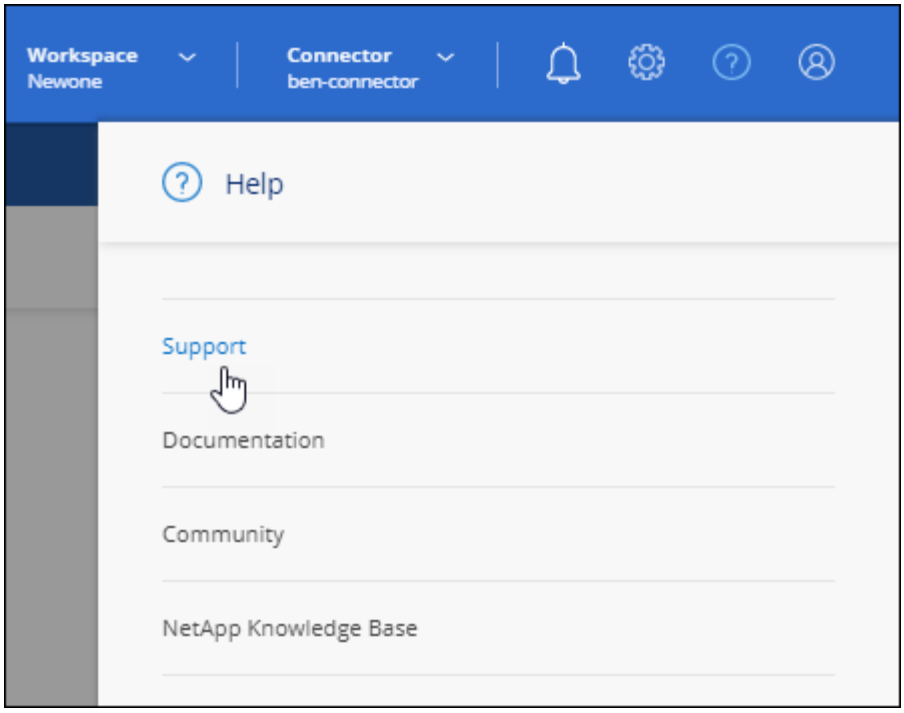
BlueXP actualiza y muestra los entornos de trabajo asociados al conector seleccionado.

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

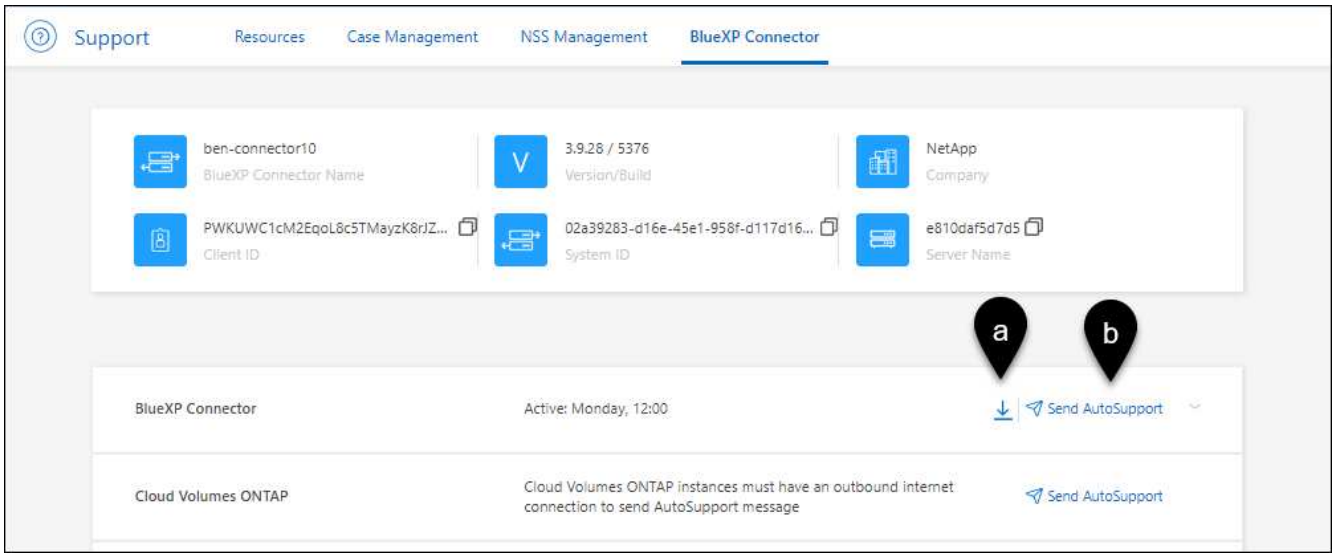
1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.



2. Seleccione **conector BlueXP**.
3. 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. Seleccione **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. El nombre de usuario para la instancia de Linux EC2 es ubuntu (para los conectores creados antes de mayo de 2023, el nombre de usuario era EC2-user).

"AWS Docs: Conéctese a su instancia de Linux"

Azure

Cuando creó la máquina virtual de Connector en Azure, especificó un nombre de usuario y optó por autenticarse con una contraseña o 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"

Requiere el uso de IMDSv2 en instancias de Amazon EC2

A partir de marzo de 2024, BlueXP ahora admite el servicio de metadatos de la instancia de Amazon EC2 versión 2 (IMDSv2) con Connector y con Cloud Volumes ONTAP (incluido el mediador para puestas en marcha de alta disponibilidad). En la mayoría de los casos, IMDSv2 se configura automáticamente en instancias de EC2 nuevas. IMDSv1 se activó antes de marzo de 2024. Si las directivas de seguridad lo requieren, es posible que deba configurar manualmente IMDSv2 en las instancias de EC2.

Acerca de esta tarea

IMDSv2 proporciona protección mejorada contra vulnerabilidades. "Obtenga más información sobre IMDSv2 en el blog de seguridad de AWS"

El servicio de metadatos de instancia (IMDS) se activa de la siguiente forma en las instancias EC2:

- Para nuevas puestas en marcha de Connector de BlueXP o mediante "Guiones Terraform", IMDSv2 está activado por defecto en la instancia EC2.
- Si inicia una nueva instancia de EC2 en AWS y, a continuación, instala manualmente el software Connector, también se habilita IMDSv2 de forma predeterminada.
- Si inicia Connector desde AWS Marketplace, IMDSv1 está habilitado de forma predeterminada. Puede configurar manualmente IMDSv2 en la instancia de EC2.
- Para los conectores existentes, IMDSv1 sigue siendo compatible, pero puede configurar manualmente IMDSv2 en la instancia EC2 si lo prefiere.
- Para Cloud Volumes ONTAP, IMDSv1 se habilita de forma predeterminada en las instancias nuevas y existentes. Puede configurar manualmente IMDSv2 en las instancias EC2 si lo prefiere.

Antes de empezar

- La versión del conector debe ser 3.9.38 o posterior.
- Cloud Volumes ONTAP debe ejecutar una de las siguientes versiones:
  - 9.12.1 P2 (o cualquier parche posterior)

- 9.13.0 P4 (o cualquier parche posterior)
- 9.13.1 o cualquier versión posterior a esta versión

- Este cambio requiere que reinicie las instancias de Cloud Volumes ONTAP.

Acerca de esta tarea

Estos pasos requieren el uso de la CLI de AWS porque debe cambiar el límite de saltos de respuesta a 3.

Pasos

1. Requerir el uso de IMDSv2 en la instancia de conector:

   a. Conéctese a la máquina virtual de Linux para el conector.

      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. El nombre de usuario para la instancia de Linux EC2 es ubuntu (para los conectores creados antes de mayo de 2023, el nombre de usuario era EC2-user).

      "AWS Docs: Conéctese a su instancia de Linux"

   b. Instale la CLI de AWS.

      "AWS Docs: Instale o actualice a la última versión de la CLI de AWS"

   c. Utilice la `aws ec2 modify-instance-metadata-options` Comando para requerir el uso de IMDSv2 y para cambiar el límite de salto de respuesta PUT a 3.

      ejemplo

      ```
      aws ec2 modify-instance-metadata-options \
          --instance-id <instance-id> \
          --http-put-response-hop-limit 3 \
          --http-tokens required \
          --http-endpoint enabled
      ```

      La `http-tokens` El parámetro establece IMDSv2 en Necesario. Cuando `http-tokens` es necesario, también debe establecer `http-endpoint` para activarlo.

2. Requerir el uso de IMDSv2 en instancias de Cloud Volumes ONTAP:

   a. Vaya a la "Consola de Amazon EC2"

   b. En el panel de navegación, selecciona **Instancias**.

   c. Seleccione una instancia de Cloud Volumes ONTAP.

   d. Seleccione **Acciones > Configuración de instancia > Modificar opciones de metadatos de instancia**.

   e. En el cuadro de diálogo **Modificar opciones de metadatos de instancia**, seleccione lo siguiente:

      - Para **servicio de metadatos de instancia**, selecciona **Habilitar**.
      - Para **IMDSv2**, selecciona **Requerido**.

- Seleccione **Guardar**.

f. Repita estos pasos para otras instancias de Cloud Volumes ONTAP, incluido el mediador HA.

g. "Pare e inicie las instancias de Cloud Volumes ONTAP"

Resultado

La instancia de conector y las instancias de Cloud Volumes ONTAP ahora están configuradas para utilizar IMDSv2.

Actualice el conector cuando utilice el modo privado

Si utiliza BlueXP en modo privado, puede actualizar Connector 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 consola basada en Web no esté disponible durante la actualización.

> Cuando usas BlueXP en modo estándar o en modo restringido, Connector actualiza automáticamente su software a la última versión, siempre y cuando tenga acceso a Internet saliente para obtener la actualización del software.

Pasos

1. Descargue el software del conector de "Sitio de soporte de NetApp".

   Asegúrese de descargar el instalador fuera de línea para redes privadas sin acceso a Internet.

2. Copie el instalador en el host Linux.
3. Asigne permisos para ejecutar el script.

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

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

4. Ejecute el script de instalación:

   ```
   sudo /path/BlueXP-Connector-offline-<version>
   ```

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

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

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.

   Deberá actualizar la ubicación de copia de seguridad de cada sistema Cloud Volumes ONTAP.

   a. Ejecute el siguiente comando desde la interfaz de línea de comandos de Cloud Volumes ONTAP para mostrar el destino actual de backup:

   ```
   system configuration backup show
   ```

   b. Ejecute el siguiente comando para actualizar la dirección IP del destino de copia de seguridad:

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

Editar los URI de un conector

Agregue y elimine el identificador uniforme de recursos (URI) de un conector.

Pasos

1. Seleccione la lista desplegable **conector** del encabezado BlueXP.
2. Seleccione **gestionar conectores**.
3. Seleccione el menú de acción de un conector y seleccione **Editar URIs**.
4. Agregue y elimine URIs y, a continuación, seleccione **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"

Quitar conectores de BlueXP

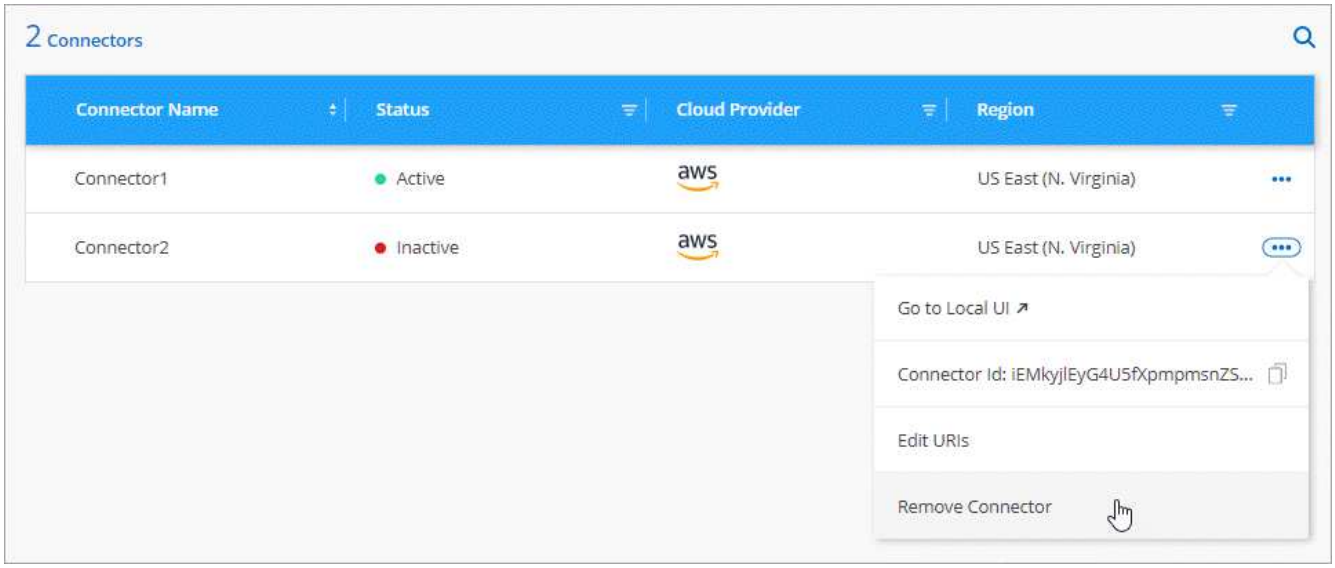
Si un conector está inactivo, puede eliminarlo de la lista de conectores de BlueXP. Puede hacerlo si ha eliminado la máquina virtual conector o si ha desinstalado el software conector.

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. Seleccione la lista desplegable **conector** del encabezado BlueXP.
2. Seleccione **gestionar conectores**.
3. Seleccione el menú de acción de un conector inactivo y seleccione **Quitar conector**.



4. Introduzca el nombre del conector que desea confirmar y, a continuación, seleccione **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 usar dependen de si instaló el conector en un host que tiene acceso a Internet (modo estándar o modo restringido) o un host en una red que no tiene acceso a Internet (modo privado).

Desinstale cuando utilice el modo estándar o el modo restringido

Los pasos a continuación le permiten desinstalar el software Connector cuando utiliza BlueXP en modo

estándar o restringido.

Pasos

1. Conéctese a la máquina virtual de Linux para el conector.
2. 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 al utilizar el modo privado

Los siguientes pasos le permiten desinstalar el software Connector cuando utiliza BlueXP en modo privado donde no hay acceso a Internet disponible.

Pasos

1. Conéctese a la máquina virtual de Linux para el conector.
2. Desde el host Linux, ejecute los siguientes comandos:

   ```
   ./opt/application/netapp/ds/cleanup.sh
   rm -rf /opt/application/netapp/ds
   ```

Instale un certificado HTTPS para obtener acceso seguro

De forma predeterminada, BlueXP utiliza un certificado autofirmado para el acceso HTTPS a la consola Web. Si así lo requiere su empresa, puede instalar un certificado firmado por una entidad de certificación (CA), la cual ofrece mejor protección de seguridad que un certificado autofirmado.

Antes de empezar

Debe crear un conector para poder cambiar la configuración de BlueXP. "Vea cómo".

Instale un certificado HTTPS

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

Pasos

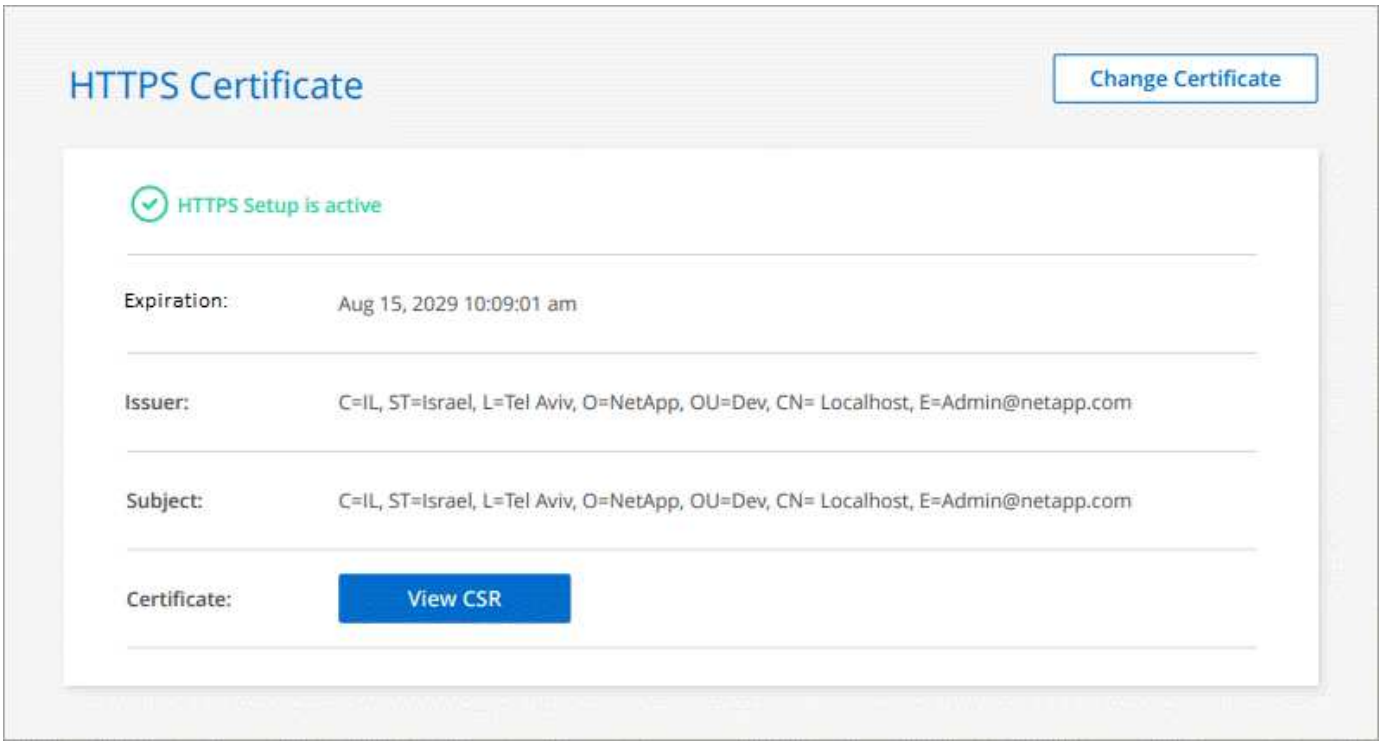
1. En la parte superior derecha de la consola BlueXP, seleccione el icono Configuración y seleccione **Configuración HTTPS**.

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	a. Introduzca el nombre de host o DNS del host del conector (su nombre común) y, a continuación, seleccione **generar CSR**. BlueXP muestra una solicitud de firma de certificado. b. Utilice la CSR para enviar una solicitud de certificado SSL a una CA. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64. c. Cargue el archivo de certificado y, a continuación, seleccione **instalar**.
Instale su propio certificado firmado por CA	a. Seleccione **instalar certificado firmado por CA**. b. Cargue el archivo de certificado y la clave privada y, a continuación, seleccione **instalar**. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.

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:



Renueve el 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, seleccione el icono Configuración y seleccione **Configuración HTTPS**.

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

2. Seleccione **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.

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.

Configuraciones admitidas

- BlueXP admite HTTP y HTTPS.
- El servidor proxy puede estar en la nube o en la red.
- BlueXP no admite servidores proxy transparentes.

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 está realizando ninguna operación antes de continuar.

Pasos

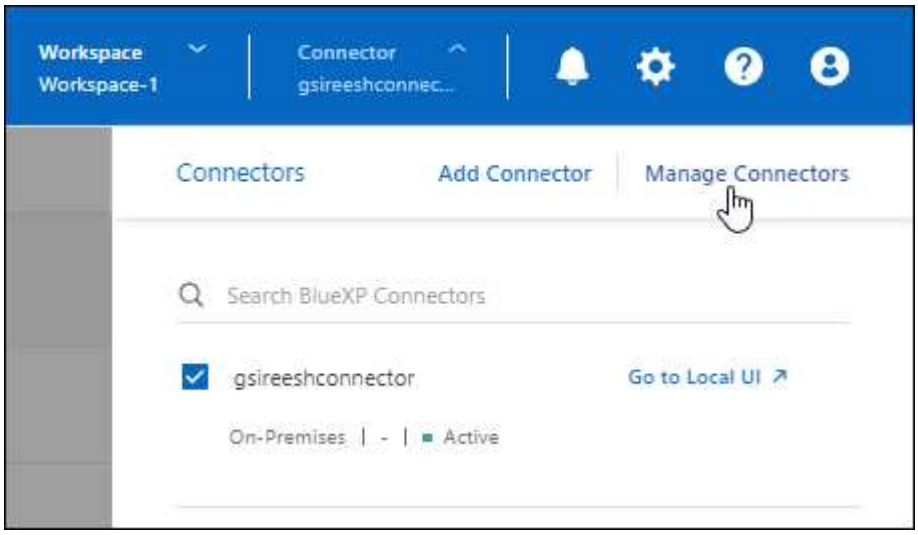
1. Navega a la página **Edit BlueXP Connector**.

   La navegación depende de si utilizas BlueXP en el modo estándar (accedes a la interfaz de BlueXP desde el sitio web de SaaS) o si utilizas BlueXP en el modo restringido o en el modo privado (accedes a la interfaz de BlueXP localmente desde el host de Connector).

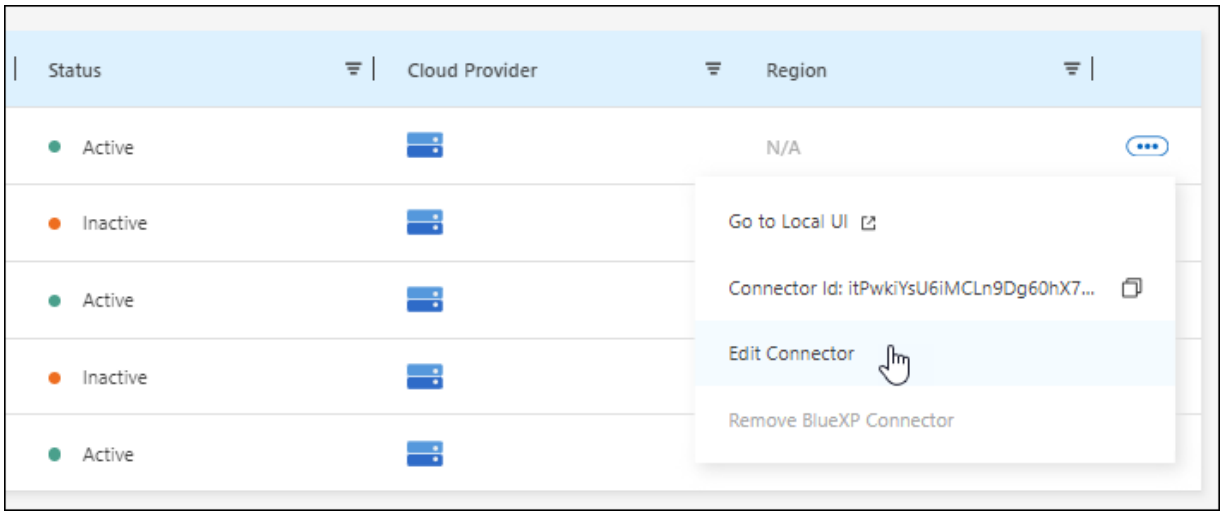
Modo estándar

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **gestionar conectores**.



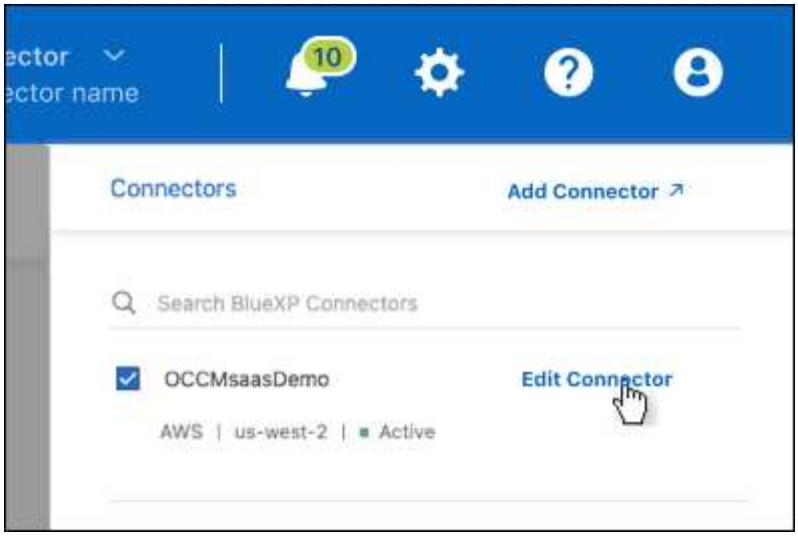
c. Seleccione el menú de acción de un conector y seleccione **Editar conector**.



Modo restringido o privado

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **Editar conector**.



2. Seleccione **Configuración de proxy HTTP**.
3. Configure el proxy:
   a. Seleccione **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 el servidor necesita autenticación básica.

      Tenga en cuenta lo siguiente:

      - El usuario puede ser un usuario local o un usuario de dominio.
      - Para un usuario de dominio, debe introducir el código ASCII para \ de la siguiente manera: Domain-name%92user-name

        Por ejemplo: netapp%92proxy

      - BlueXP no admite contraseñas que incluyan el carácter @.
   d. Seleccione **Guardar**.

Habilite el tráfico de API directo

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

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

"Obtenga más información sobre el uso de un enlace privado de Azure o extremos de servicio con Cloud Volumes ONTAP"

Pasos

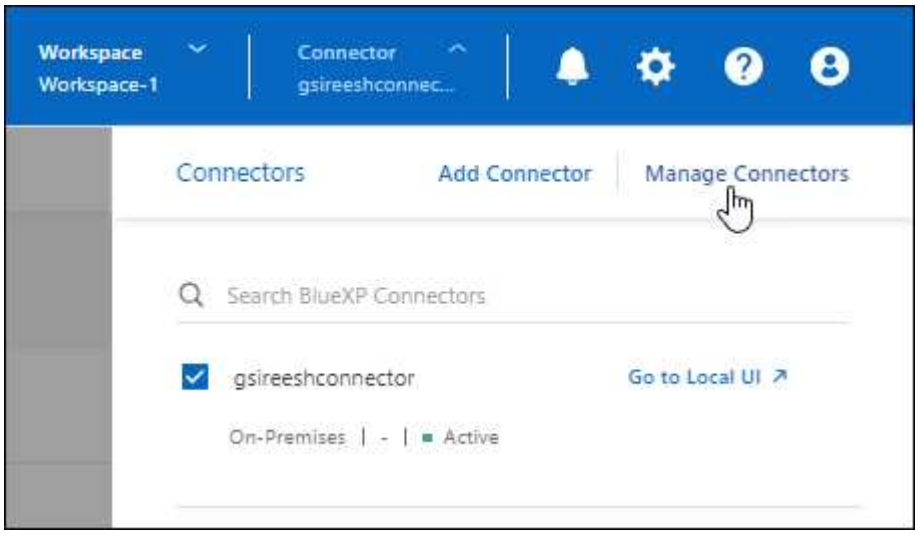
1. Navega a la página **Edit BlueXP Connector**:

La navegación depende de si utilizas BlueXP en el modo estándar (accedes a la interfaz de BlueXP desde el sitio web de SaaS) o si utilizas BlueXP en el modo restringido o en el modo privado (accedes a la interfaz de BlueXP localmente desde el host de Connector).

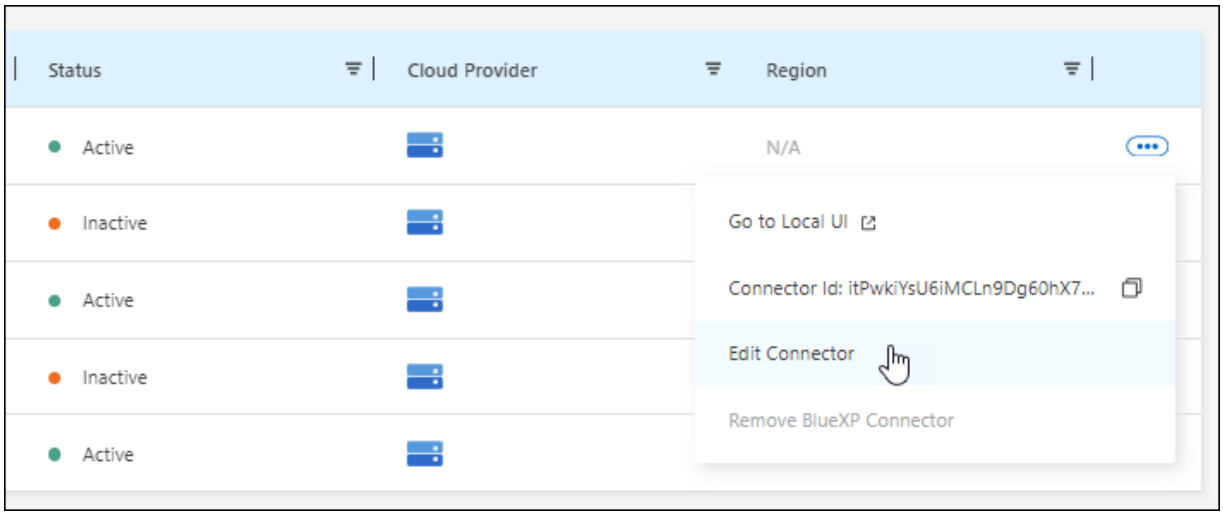
Modo estándar

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **gestionar conectores**.



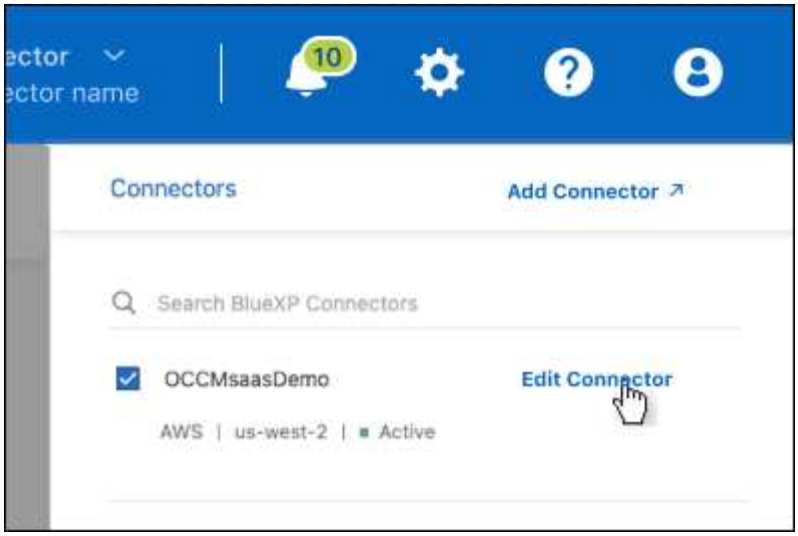
c. Seleccione el menú de acción de un conector y seleccione **Editar conector**.



Modo restringido o privado

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **Editar conector**.



2. Selecciona **Soporte Direct API Traffic**.
3. Seleccione la casilla de verificación para activar la opción y, a continuación, seleccione **Guardar**.

Configuración predeterminada del conector

Es posible que desee obtener más información sobre la configuración del 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 Ubuntu 22,04 LTS.

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

- El nombre de usuario para la instancia de Linux EC2 es ubuntu (para los conectores creados antes de mayo de 2023, el nombre de usuario era 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 Ubuntu 22,04 LTS.

  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 Connector de BlueXP, tenga en cuenta lo siguiente:

- La instancia del equipo virtual es n2-standard-4.
- El sistema operativo de la imagen es Ubuntu 22,04 LTS.

  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 el 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 el acceso HTTPS

Credenciales y suscripciones

AWS

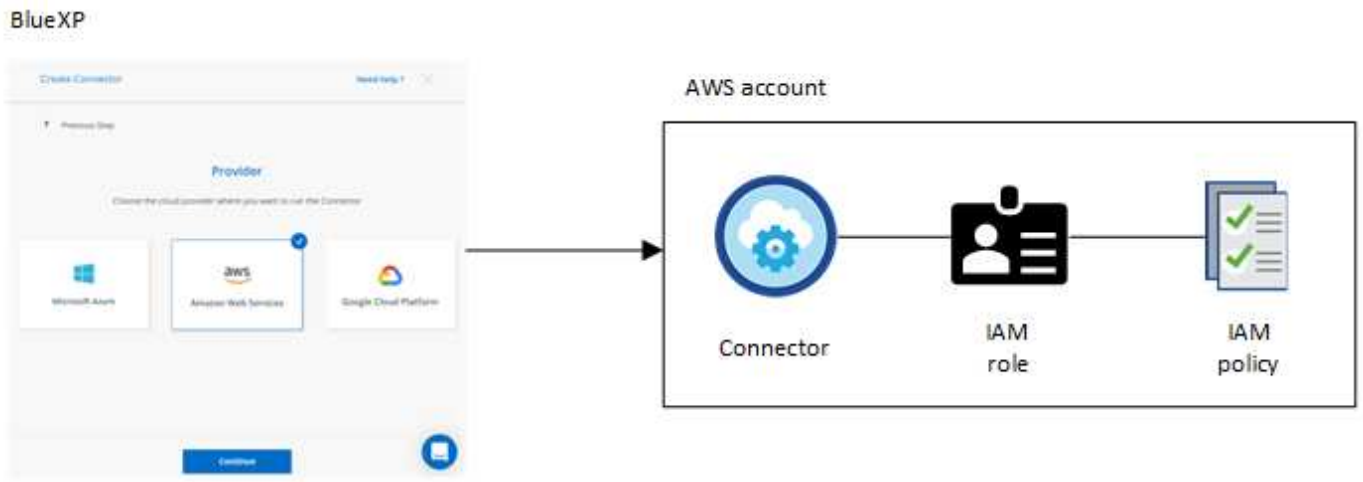
Obtenga más información acerca de los permisos y credenciales de AWS

Descubre cómo BlueXP utiliza las credenciales de AWS para realizar acciones en tu nombre y cómo esas credenciales están asociadas a las suscripciones del mercado. Comprender estos detalles puede resultar útil a la hora de gestionar las credenciales de una o más cuentas de AWS en BlueXP. Por ejemplo, quizás quieras saber cuándo añadir más credenciales de AWS a BlueXP.

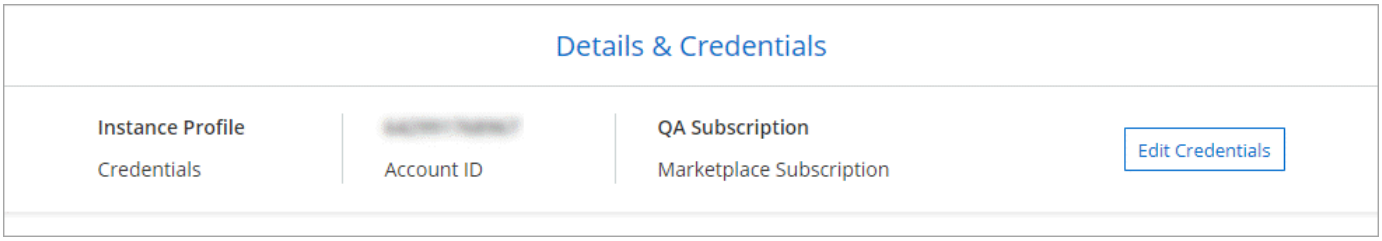
Credenciales iniciales de AWS

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".



Si creas un nuevo entorno de trabajo para Cloud Volumes ONTAP, BlueXP selecciona estas credenciales de AWS de forma predeterminada:



Puede implementar todos sus sistemas Cloud Volumes ONTAP con las credenciales iniciales de AWS o bien añadir credenciales adicionales.

Credenciales adicionales de AWS

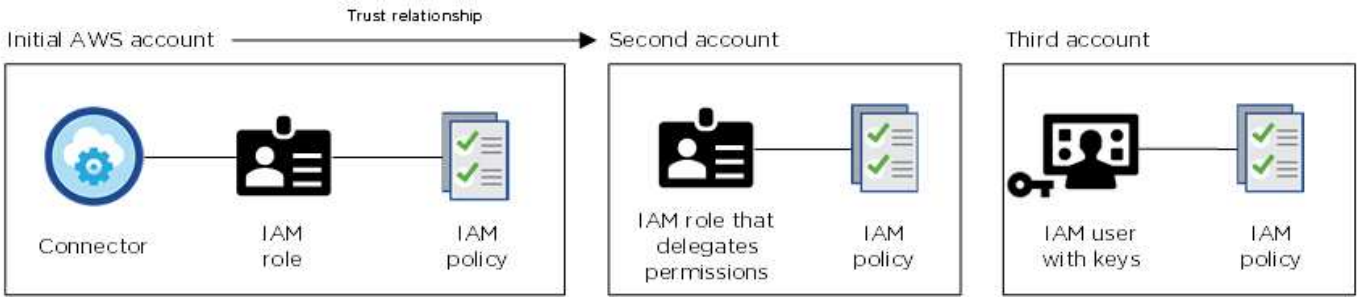
Existen dos formas de añadir credenciales de AWS adicionales:

- Puede agregar credenciales de AWS a un conector existente
- Puede añadir credenciales de AWS directamente a BlueXP

Revise las secciones siguientes para obtener más información.

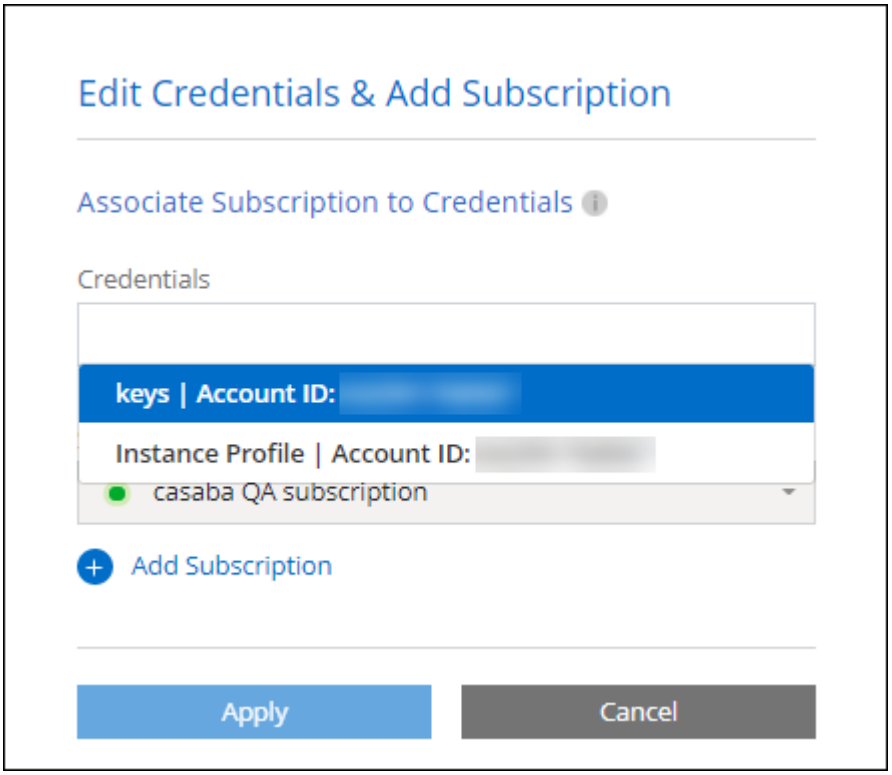
Agregar credenciales de AWS a un conector existente

Si desea usar BlueXP con cuentas adicionales de AWS, puede proporcionar claves de 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:



A continuación, se agregarían las credenciales de cuenta a BlueXP especificando el nombre de recurso de Amazon (ARN) del rol IAM o las claves de AWS del usuario de IAM.

Por ejemplo, es posible cambiar entre credenciales al crear un nuevo entorno de trabajo Cloud Volumes ONTAP:



"Aprenda a añadir credenciales de AWS a un conector existente."

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.

- "Aprenda a añadir credenciales de AWS a BlueXP para Amazon FSX para ONTAP"
- "Aprenda a añadir credenciales de AWS a BlueXP para crear un conector"

Credenciales y suscripciones de Marketplace

Las credenciales que añadas a un conector deben estar asociadas a una suscripción de AWS Marketplace para que puedas pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO) o a través de un contrato anual, así como para utilizar otros servicios de BlueXP.

"Aprenda a asociar una suscripción a AWS".

Tenga en cuenta lo siguiente acerca de las credenciales de AWS y las suscripciones al mercado:

- Solo se puede asociar una suscripción de AWS Marketplace a un conjunto de credenciales de AWS
- Puede reemplazar una suscripción existente de Marketplace por una nueva

PREGUNTAS FRECUENTES

Las siguientes preguntas están relacionadas con las credenciales y suscripciones.

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

Como se describe en las secciones anteriores, BlueXP le permite proporcionar credenciales de AWS de varias formas: Un rol de IAM asociado a la instancia de Connector, asumiendo un rol de 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.

¿Puedo cambiar la suscripción de AWS Marketplace para entornos de trabajo de Cloud Volumes ONTAP?

Sí, puedes. Al cambiar la suscripción de AWS Marketplace asociada a un conjunto de credenciales, todos los entornos de trabajo de Cloud Volumes ONTAP existentes y nuevos se cargarán con la nueva suscripción.

"Aprenda a asociar una suscripción a AWS".

¿Puedo añadir varias credenciales de AWS, cada una con diferentes suscripciones del mercado?

Todas las credenciales de AWS que pertenezcan a la misma cuenta de AWS se asociarán a la misma suscripción de AWS Marketplace.

Si tiene varias credenciales de AWS que pertenecen a diferentes cuentas de AWS, esas credenciales se pueden asociar con la misma suscripción de AWS Marketplace o con diferentes suscripciones.

¿Puedo mover entornos de trabajo existentes de Cloud Volumes ONTAP a otra cuenta de AWS?

No, no es posible mover los recursos de AWS asociados con su entorno de trabajo de Cloud Volumes ONTAP a una cuenta de AWS diferente.

¿Cómo funcionan las credenciales en las implementaciones del mercado y en las instalaciones?

En las secciones anteriores se describe el método de implementación recomendado para el conector, que es de BlueXP. También puede poner en marcha un conector en AWS desde AWS Marketplace y puede instalar manualmente el software del conector en su propio host Linux.

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Solo tiene que crear y configurar manualmente el rol IAM y, a continuación, proporcionar permisos para cualquier cuenta adicional.

En las implementaciones locales, no se puede configurar la función de IAM para el sistema BlueXP, pero se pueden proporcionar permisos con las claves de acceso de AWS.

Para aprender a configurar los permisos, consulte las siguientes páginas:

- Modo estándar
  - "Configure los permisos para una puesta en marcha de AWS Marketplace"

    - "Configure los permisos para implementaciones en las instalaciones"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

Gestiona las credenciales y las suscripciones del mercado 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 a AWS Marketplace, 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 adicionales a un conector

Añada credenciales de AWS adicionales a un conector para que tenga los permisos necesarios para gestionar 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.

Si acaba de empezar a utilizar BlueXP, "Descubra cómo BlueXP usa credenciales y permisos 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, seleccione **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, seleccione el icono Configuración y seleccione **credenciales**.

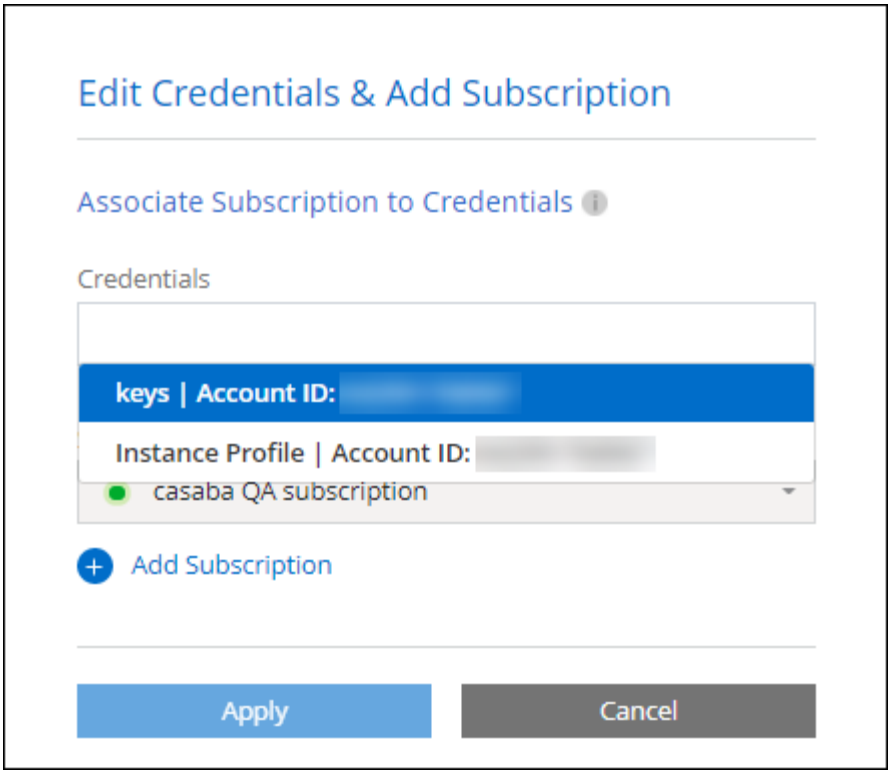
3. En la página **credenciales de cuenta**, seleccione **Agregar credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Servicios Web de Amazon > conector**.
   b. **Definir credenciales**: Proporcione el ARN (nombre de recurso de Amazon) de una función de IAM 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 servicios de BlueXP a una tarifa por hora (PAYGO) o con un contrato anual, las credenciales de AWS deben estar asociadas a una suscripción de AWS Marketplace.

   d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

Ahora puede cambiar a un conjunto de credenciales diferente de la página Details y Credentials al crear un nuevo entorno de trabajo:



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 a la capa SaaS BlueXP asumir la función.

Pasos

1. Vaya a la consola IAM de la cuenta de destino.
2. En Access Management, seleccione **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, seleccione el icono Configuración y seleccione **credenciales**.

2. En la página **credenciales de cuenta**, seleccione **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 sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

Ahora puede utilizar las credenciales al crear un conector nuevo.

Añada credenciales a BlueXP para Amazon FSX para ONTAP

Para obtener más información, consulte "Documentación de BlueXP para Amazon FSX para ONTAP"

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 mediante un contrato anual, y utilizar otros servicios de BlueXP.

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 cambiar la suscripción de AWS Marketplace asociada con las credenciales de AWS.

  La sustitución de la suscripción actual del mercado por una nueva suscripción cambia la suscripción del mercado para cualquier entorno de trabajo existente de Cloud Volumes ONTAP y todos los nuevos entornos de trabajo.

Antes de empezar

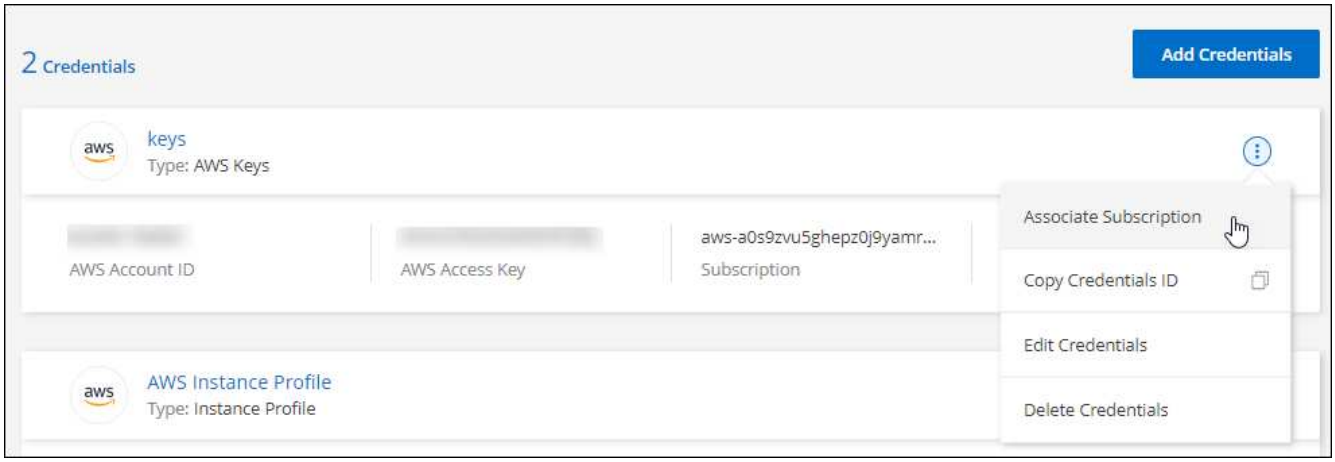
Debe crear un conector para poder cambiar la configuración de BlueXP. "Aprenda a crear un conector".

Pasos

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

2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y seleccione **asociado**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos del AWS Marketplace:

   a. Seleccione **Ver opciones de compra**.

   b. Seleccione **Suscribirse**.

   c. Seleccione **Configurar su cuenta**.

      Se le redirigirá al sitio web de BlueXP.

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

      - Seleccione las cuentas de BlueXP con 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.

      - Seleccione **Guardar**.

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

   Suscríbete a BlueXP desde AWS Marketplace

Asocie una suscripción existente a su cuenta

Cuando te suscribes a BlueXP desde AWS Marketplace, el último paso del proceso es asociar la suscripción a tus cuentas de BlueXP desde el sitio web de BlueXP. Si no has completado este paso, no podrás usar la

suscripción con tu cuenta de BlueXP.

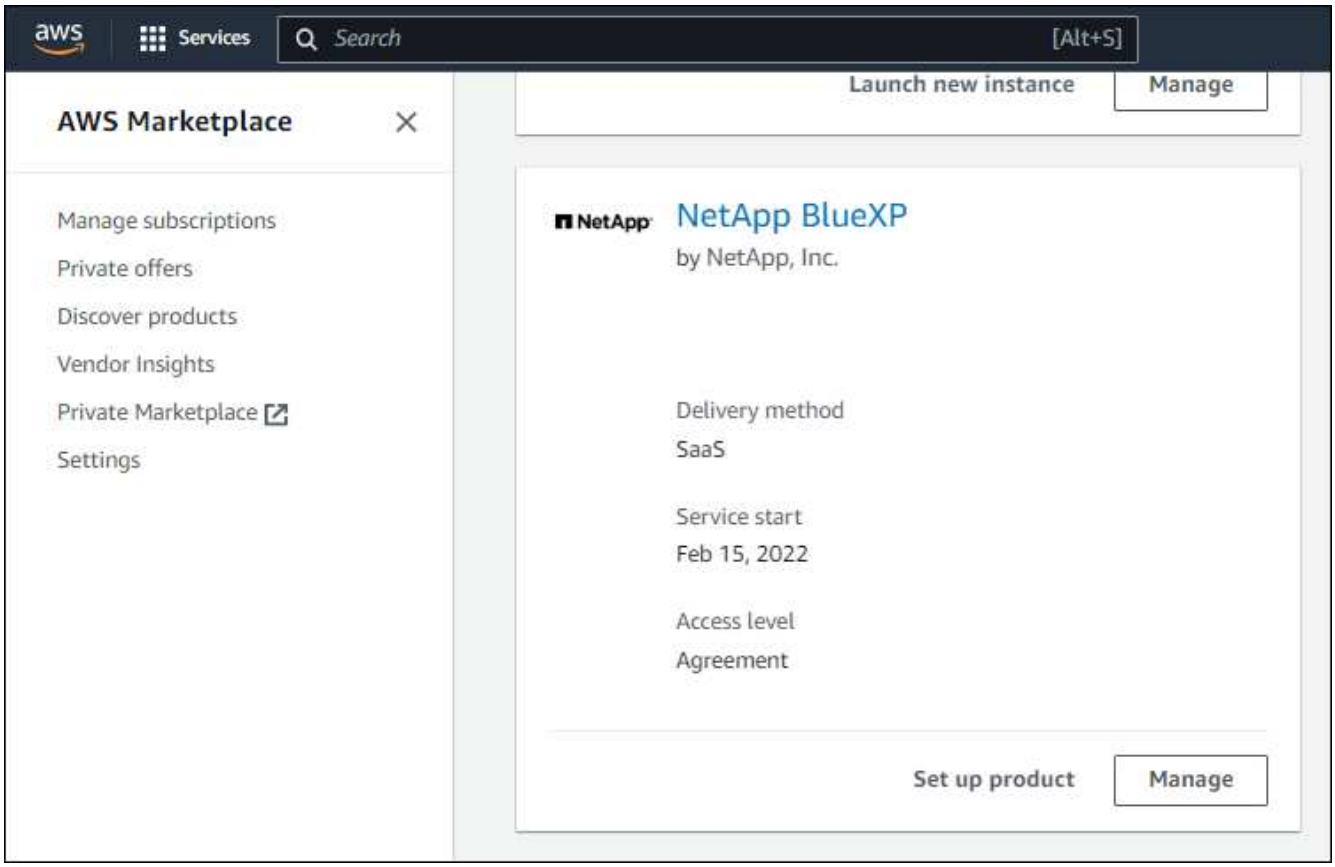
Sigue los pasos que aparecen a continuación si te suscribiste a BlueXP desde AWS Marketplace, pero te has perdido el paso para asociar la suscripción a tu cuenta.

Pasos

1. Ve a la cartera digital de BlueXP para confirmar que no has asociado tu suscripción a tu cuenta de BlueXP.
   a. En el menú de navegación de BlueXP, seleccione **Gobierno > cartera digital**.
   b. Seleccione **Suscripciones**.
   c. Comprueba que no aparezca tu suscripción a BlueXP.

      Solo verá las suscripciones asociadas a la cuenta que está viendo actualmente. Si no ve su suscripción, continúe con los siguientes pasos.

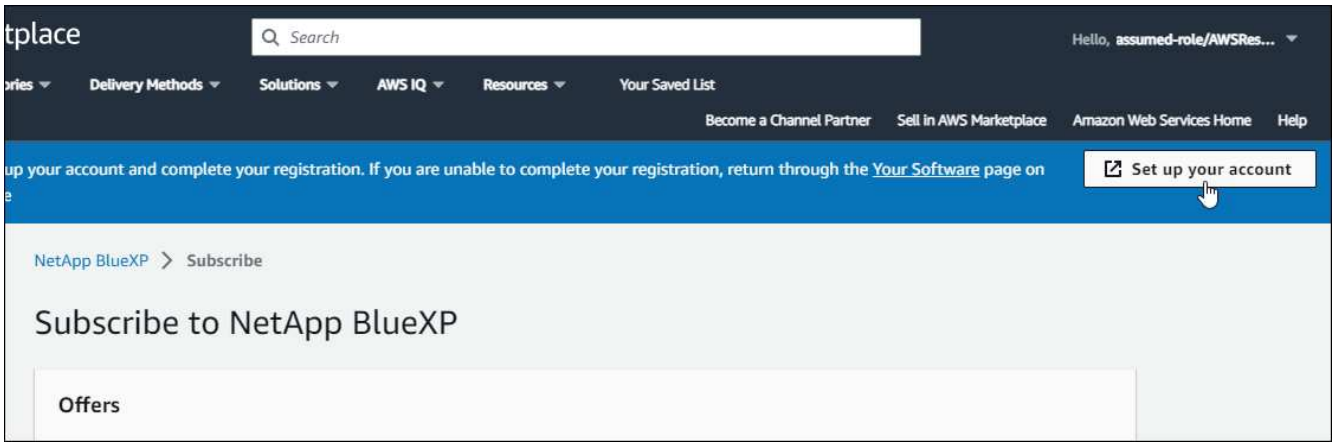
2. Inicie sesión en la consola de AWS y vaya a * Suscripciones de AWS Marketplace *.
3. Encuentra la suscripción a NetApp BlueXP.



4. Seleccione **Set up product**.

   La página de oferta de suscripción debe cargarse en una nueva pestaña o ventana del navegador.

5. Seleccione **Configurar su cuenta**.



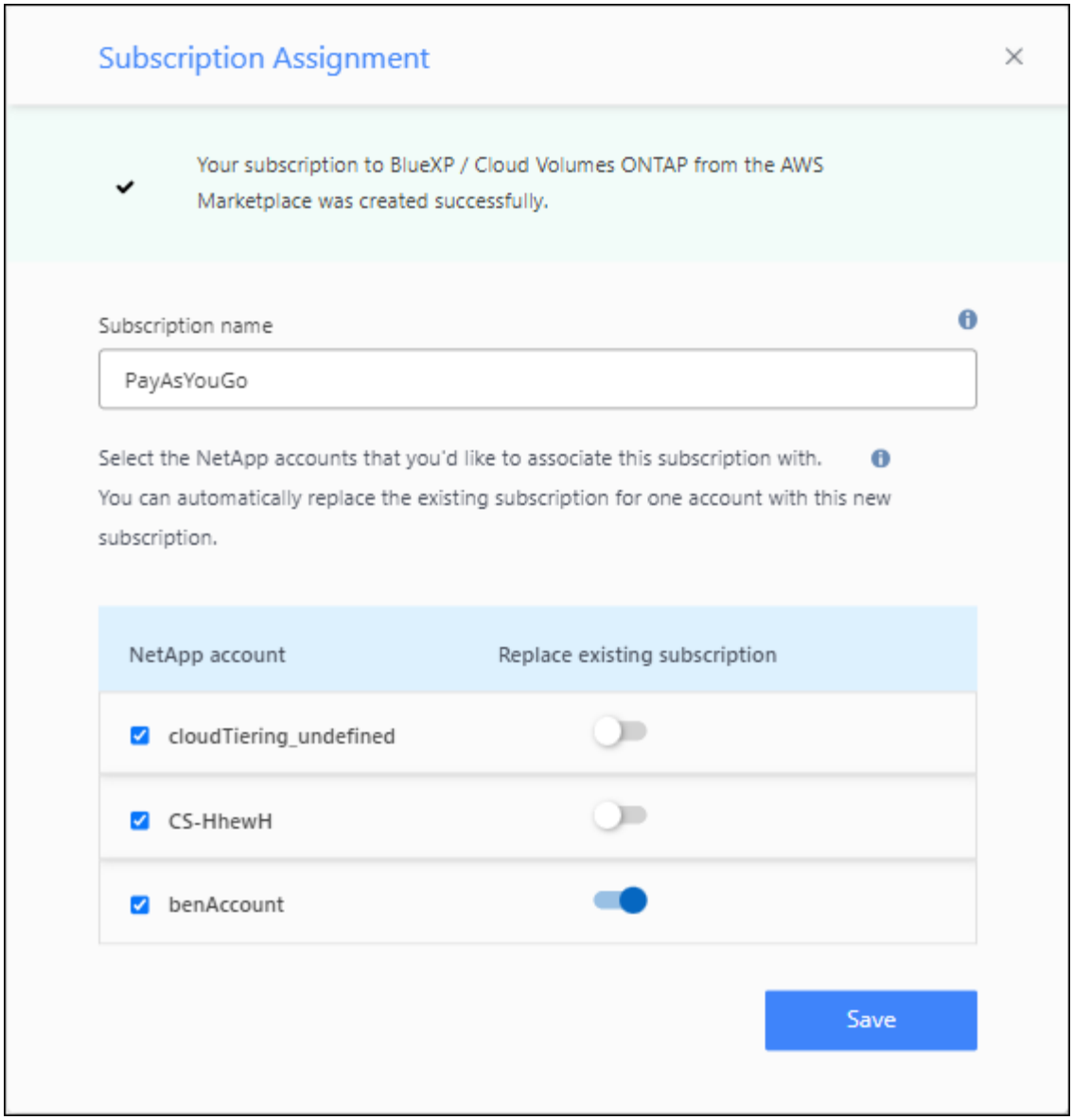
La página **Suscripción** en netapp.com debe cargarse en una nueva pestaña o ventana del navegador.

Ten en cuenta que es posible que se te pida iniciar sesión en BlueXP primero.

6. Desde la página **asignación de suscripción**:
   - Seleccione las cuentas de BlueXP con 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.

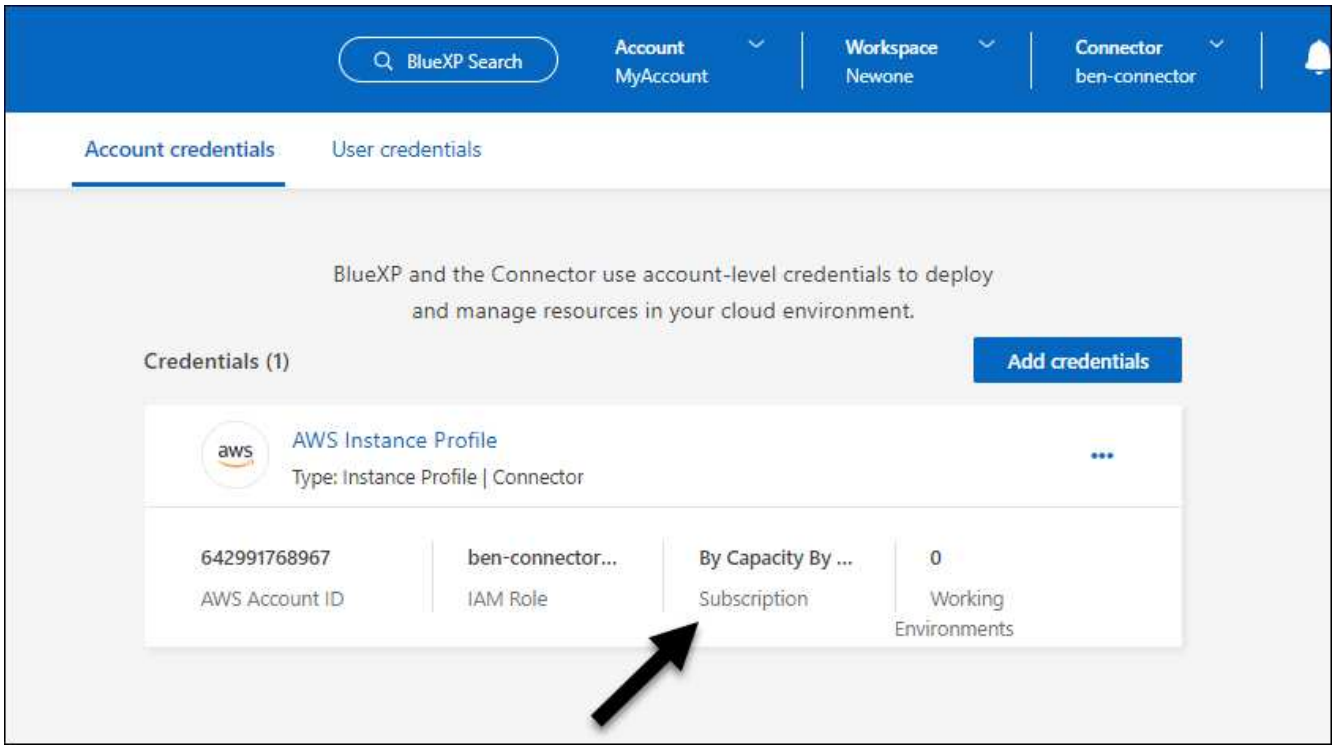
     BlueXP reemplaza la suscripción existente para todas las credenciales de la cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

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



7. Ve a la cartera digital de BlueXP para confirmar que la suscripción está asociada a tu cuenta de BlueXP.
   a. En el menú de navegación de BlueXP, seleccione **Gobierno > cartera digital**.
   b. Seleccione **Suscripciones**.
   c. Comprueba que aparezca tu suscripción a BlueXP.
8. Confirme que la suscripción está asociada a sus credenciales de AWS.
   a. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
   b. En la página **Account credentials**, verifique que la suscripción esté asociada con sus credenciales de AWS.

      Veamos un ejemplo.



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, seleccione el icono Configuración y seleccione **credenciales**.
2. En la página **credenciales de cuenta**, seleccione el menú de acción para un conjunto de credenciales y, a continuación, seleccione **Editar credenciales**.
3. Realice los cambios necesarios y, a continuación, seleccione **aplicar**.

Eliminar 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, seleccione el icono Configuración y seleccione **credenciales**.
2. En la página **credenciales de cuenta**, seleccione el menú de acción para un conjunto de credenciales y, a continuación, seleccione **Eliminar credenciales**.

3. Seleccione **Eliminar** para confirmar.

Azure

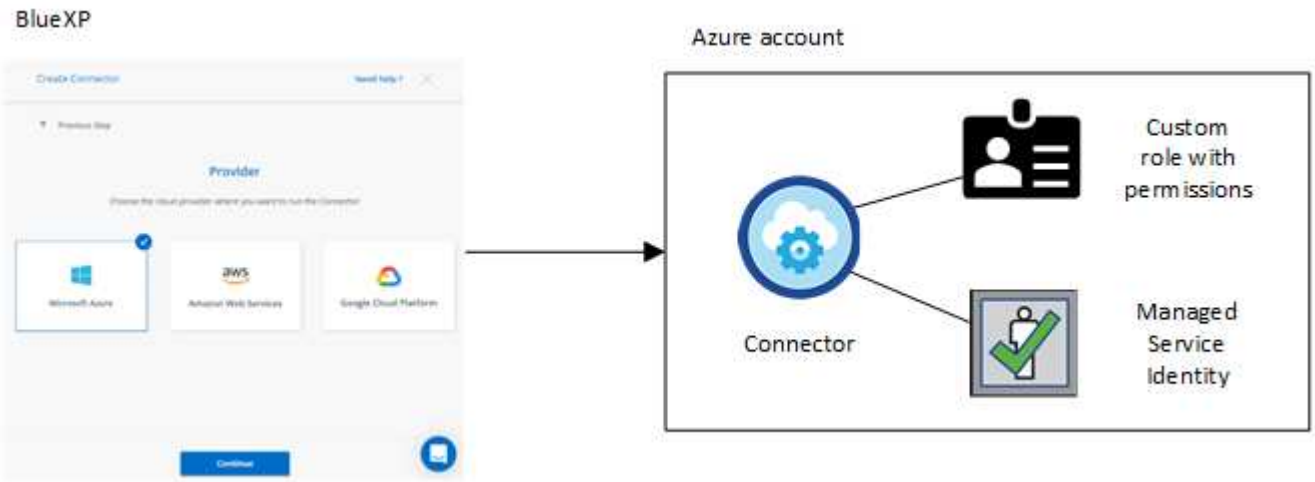
Obtenga más información acerca de credenciales y permisos de Azure

Descubre cómo BlueXP utiliza las credenciales de Azure para realizar acciones en tu nombre y cómo esas credenciales están asociadas a las suscripciones del mercado. Comprender estos detalles puede resultar útil cuando gestionas las credenciales de una o más suscripciones a Azure. Por ejemplo, quizás quieras saber cuándo añadir credenciales de Azure adicionales en BlueXP.

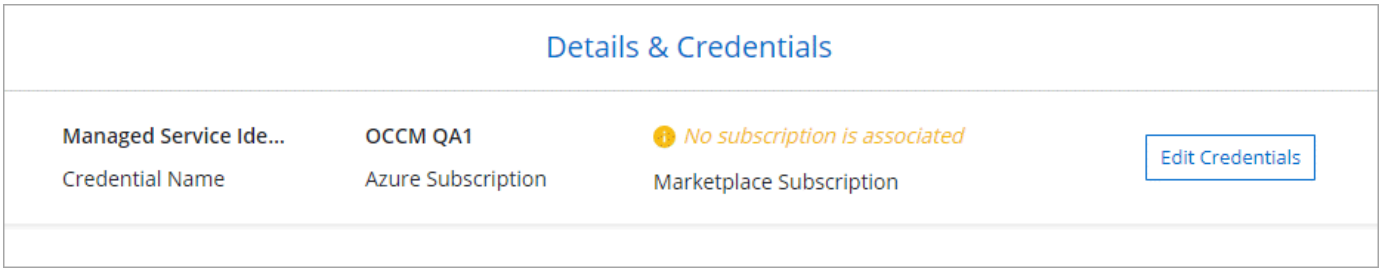
Credenciales iniciales de Azure

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".



Si creas un nuevo entorno de trabajo para Cloud Volumes ONTAP, BlueXP selecciona estas credenciales de Azure de forma predeterminada:



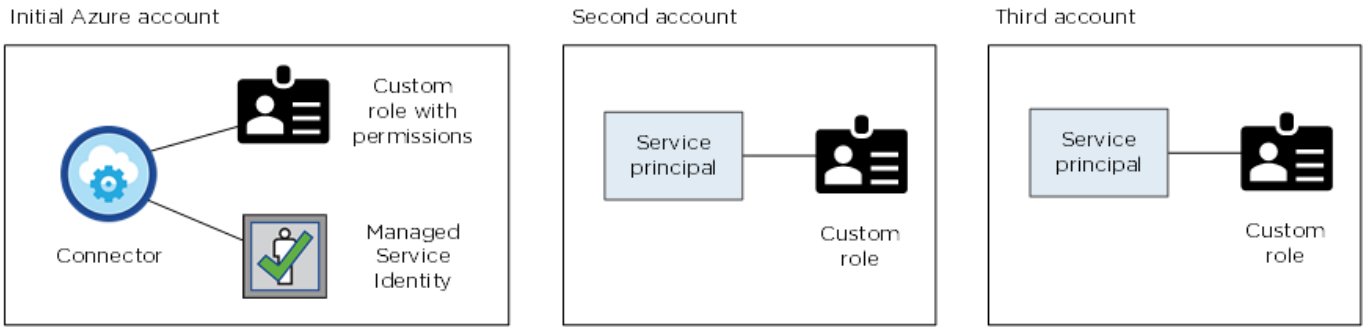
Puede poner en marcha todos los sistemas de Cloud Volumes ONTAP con las credenciales iniciales de Azure o bien añadir credenciales adicionales.

Suscripciones adicionales de Azure para una identidad gestionada

La identidad administrada asignada por el sistema asignada a la máquina virtual del conector 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".

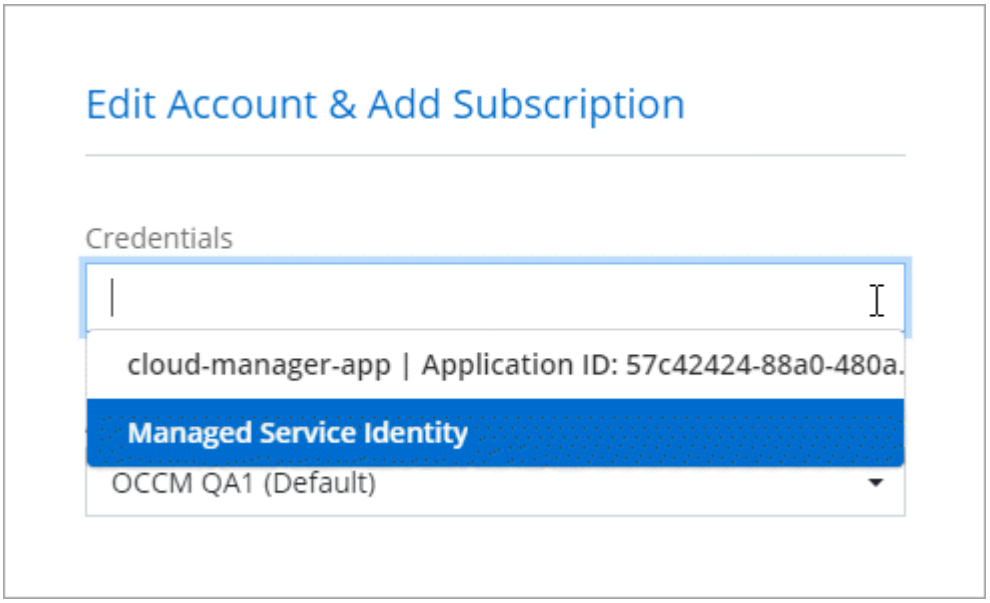
Credenciales adicionales de Azure

Si desea utilizar diferentes credenciales de Azure con BlueXP, debe conceder los permisos necesarios mediante "Creación y configuración de un principal de servicio en Microsoft Entra ID" Para cada cuenta de Azure. La siguiente imagen muestra dos cuentas adicionales, cada una configurada con una función personalizada y principal de servicio que proporciona permisos:



Entonces lo haría "Agregue las credenciales de cuenta a BlueXP" Proporcionando detalles acerca del director de servicio de AD.

Por ejemplo, es posible cambiar entre credenciales al crear un nuevo entorno de trabajo Cloud Volumes ONTAP:



Credenciales y suscripciones de Marketplace

Las credenciales que añadas a un conector deben estar asociadas a una suscripción a Azure Marketplace para que puedas pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO) o a través de un contrato anual, y para utilizar otros servicios de BlueXP.

"Aprenda a asociar una suscripción a Azure".

Tenga en cuenta lo siguiente acerca de las credenciales de Azure y las suscripciones a Marketplace:

- Solo puede asociar una suscripción de Azure Marketplace a un conjunto de credenciales de Azure
- Puede reemplazar una suscripción existente de Marketplace por una nueva

PREGUNTAS FRECUENTES

La siguiente pregunta está relacionada con las credenciales y suscripciones.

¿Puedo cambiar la suscripción a Azure Marketplace para entornos de trabajo de Cloud Volumes ONTAP?

Sí, puedes. Al cambiar la suscripción de Azure Marketplace asociada a un conjunto de credenciales de Azure, todos los entornos de trabajo de Cloud Volumes ONTAP existentes y nuevos se cargarán con la nueva suscripción.

"Aprenda a asociar una suscripción a Azure".

¿Puedo agregar varias credenciales de Azure, cada una con diferentes suscripciones del mercado?

Todas las credenciales de Azure que pertenezcan a la misma suscripción de Azure se asociarán a la misma suscripción de Azure Marketplace.

Si tiene varias credenciales de Azure que pertenecen a diferentes suscripciones de Azure, esas credenciales se pueden asociar con la misma suscripción de Azure Marketplace o con diferentes suscripciones de Marketplace.

¿Puedo mover entornos de trabajo existentes de Cloud Volumes ONTAP a una suscripción diferente a Azure?

No, no es posible mover los recursos de Azure asociados con su entorno de trabajo de Cloud Volumes ONTAP a una suscripción de Azure diferente.

¿Cómo funcionan las credenciales en las implementaciones del mercado y en las instalaciones?

En las secciones anteriores se describe el método de implementación recomendado para el conector, que es de BlueXP. También puede poner en marcha un conector en Azure desde Azure Marketplace y puede instalar el software del conector en su propio host Linux.

Si utiliza Marketplace, puede proporcionar permisos asignando un rol personalizado a la VM de Connector y a una identidad administrada asignada por el sistema, o puede usar un principal de servicio de Microsoft Entra.

Para implementaciones en las instalaciones, no puede configurar una identidad administrada para el conector, pero puede proporcionar permisos utilizando un director de servicio.

Para aprender a configurar los permisos, consulte las siguientes páginas:

- Modo estándar
  - "Configure los permisos para una puesta en marcha de Azure Marketplace"
  - "Configure los permisos para implementaciones en las instalaciones"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

Gestiona las credenciales de Azure y las suscripciones al mercado para BlueXP

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

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.

Descripción general

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.

Asocie suscripciones adicionales de Azure a una identidad gestionada

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

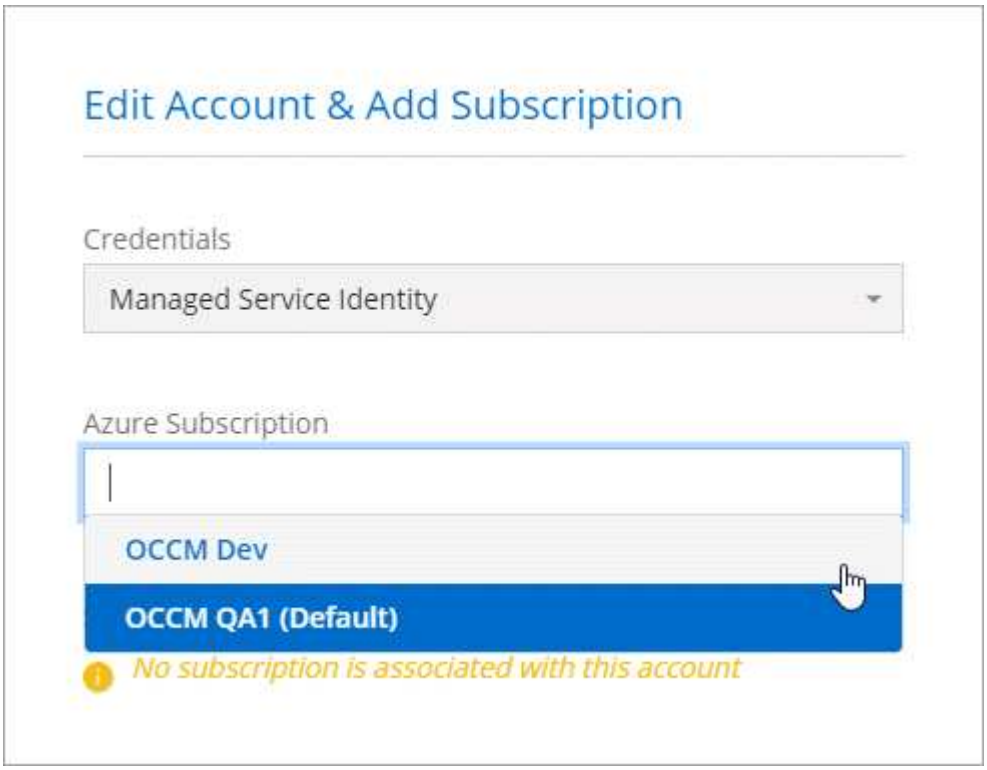
1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar Cloud Volumes ONTAP.
3. Seleccionar **Control de acceso (IAM)**.
   a. Seleccione **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos: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

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

      - Asigne acceso a una **máquina virtual**.
      - Seleccione la suscripción en la que se creó la máquina virtual Connector.
      - Seleccione la máquina virtual conector.
      - Seleccione **Guardar**.
4. Repita estos pasos para suscripciones adicionales.

Resultado

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



Añada 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".

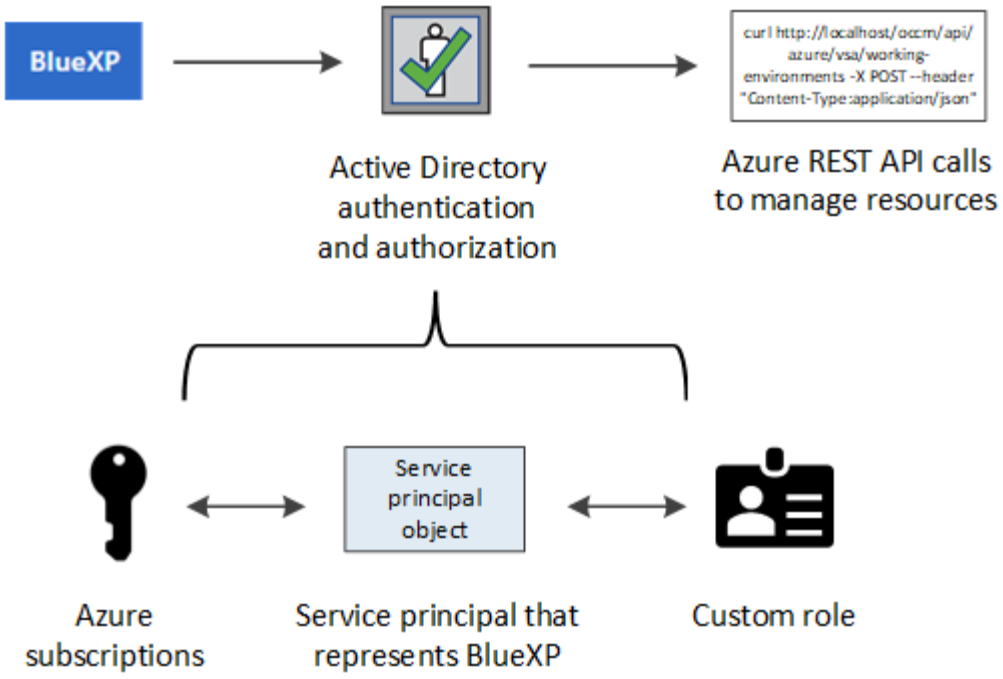
Si desea implementar Cloud Volumes ONTAP con credenciales *DIFERENTE* de Azure, debe otorgar los permisos necesarios creando y configurando un principal de servicio en Microsoft Entra ID para cada cuenta de Azure. A continuación, puede agregar las nuevas credenciales a BlueXP.

Conceda permisos de Azure con un director de servicio

BlueXP necesita permisos para realizar acciones en Azure. Puedes conceder los permisos necesarios a una cuenta de Azure creando y configurando un principal de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que necesita BlueXP.

Acerca de esta tarea

La siguiente imagen muestra cómo BlueXP obtiene permisos para realizar operaciones en Azure. Un objeto principal de servicio, vinculado a una o varias suscripciones de Azure, representa a BlueXP en Microsoft Entra ID y se asigna a un rol personalizado que permite los permisos requeridos.



Pasos

1. Cree una aplicación Microsoft Entra.
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 Microsoft Entra

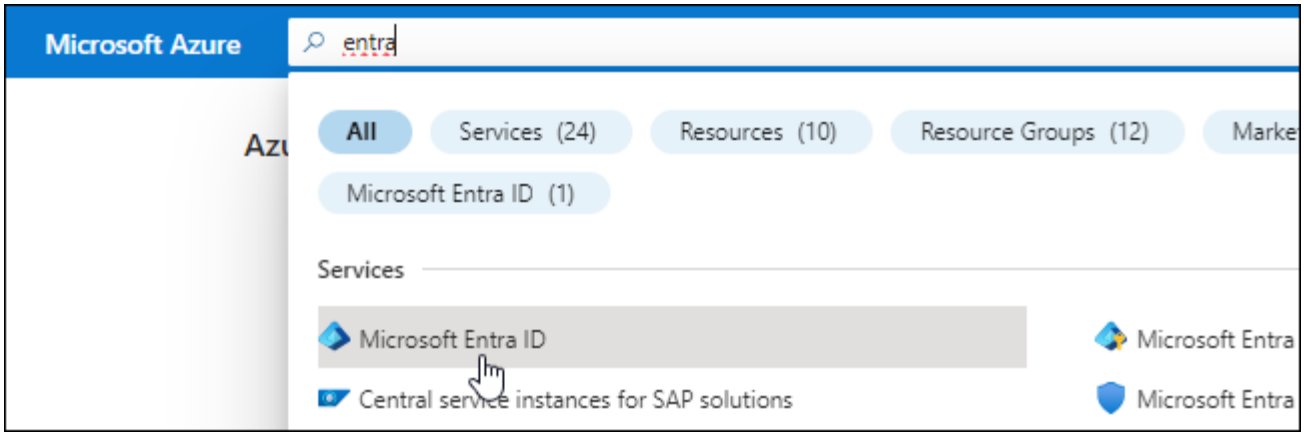
Crea una aplicación de Microsoft Entra y una entidad de servicio que BlueXP pueda utilizar para el control de acceso basado en roles.

Pasos

1. Asegúrese de tener permisos en Azure para crear una aplicación de Active Directory y para asignar la aplicación a un rol.

   Para obtener más información, consulte "Documentación de Microsoft Azure: Permisos necesarios"

2. Desde el portal de Azure, abra el servicio **Microsoft Entra ID**.



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. 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.
6. Seleccione **Registrar**.

   Ha creado la aplicación AD y el director de servicio.

Resultado

Ha creado la aplicación AD y el director de servicio.

Asigne 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:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

   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.

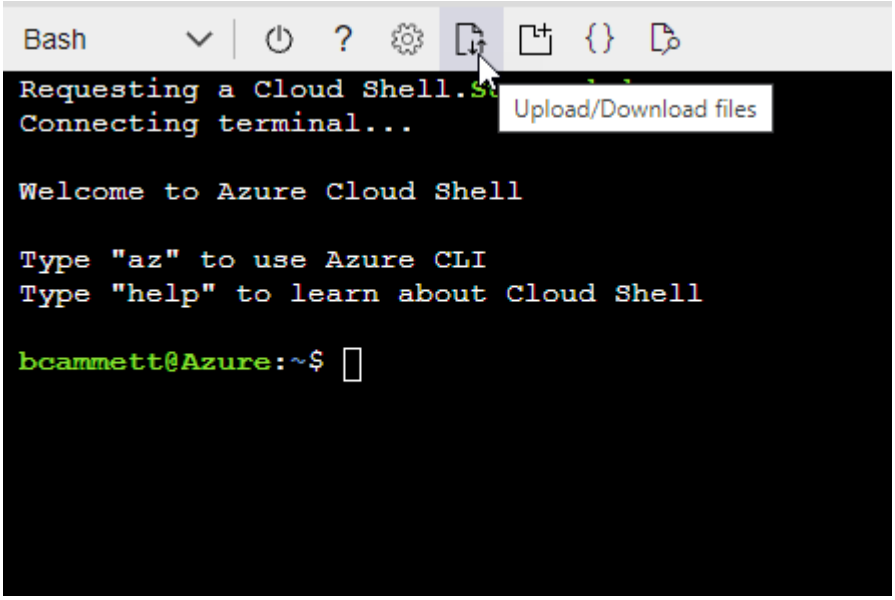
      ejemplo

```
"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**.

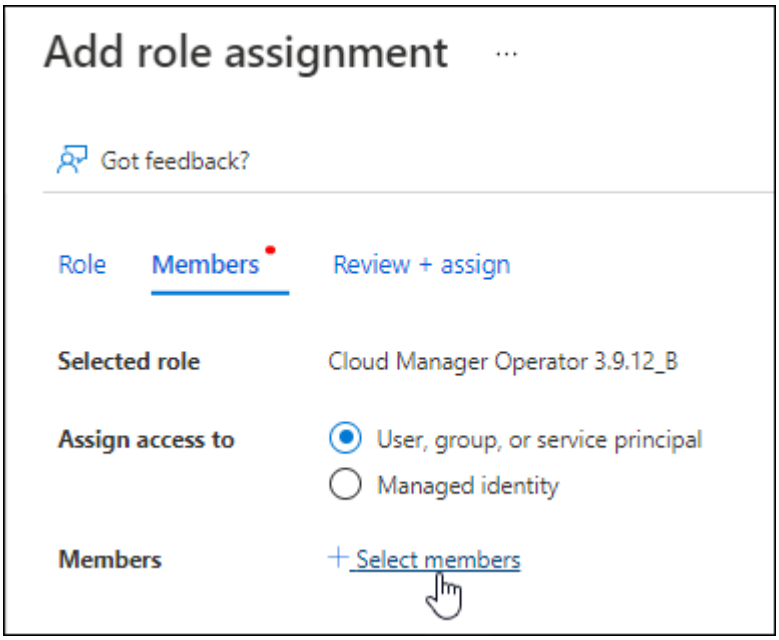
b. Seleccione la suscripción.

c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.

d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.

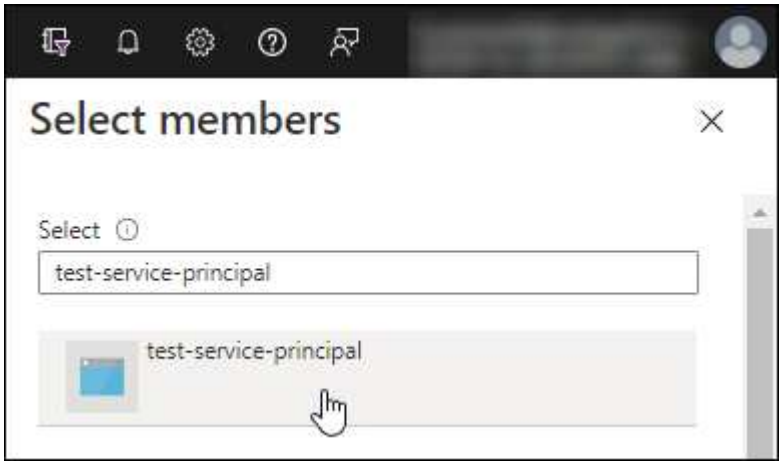
e. En la ficha **Miembros**, realice los siguientes pasos:

- Mantener seleccionado **Usuario, grupo o principal de servicio**.
- Seleccione **Seleccionar miembros**.



- Busque el nombre de la aplicación.

  Veamos un ejemplo:



- Seleccione la aplicación y seleccione **Seleccionar**.
- Seleccione **Siguiente**.

f. Seleccione **revisar + asignar**.

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

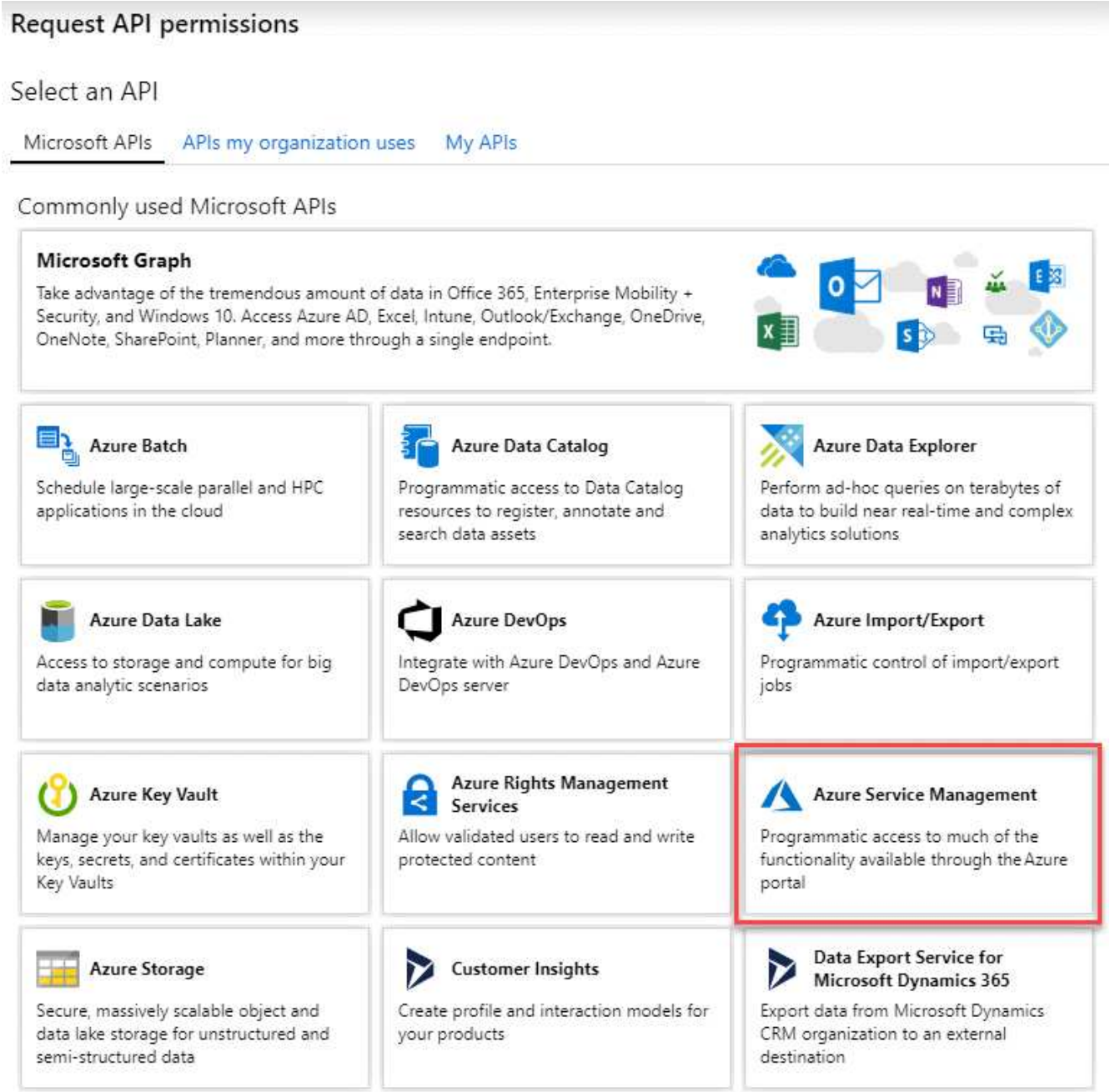
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. BlueXP le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

Añada permisos de API de administración de servicios de Windows Azure

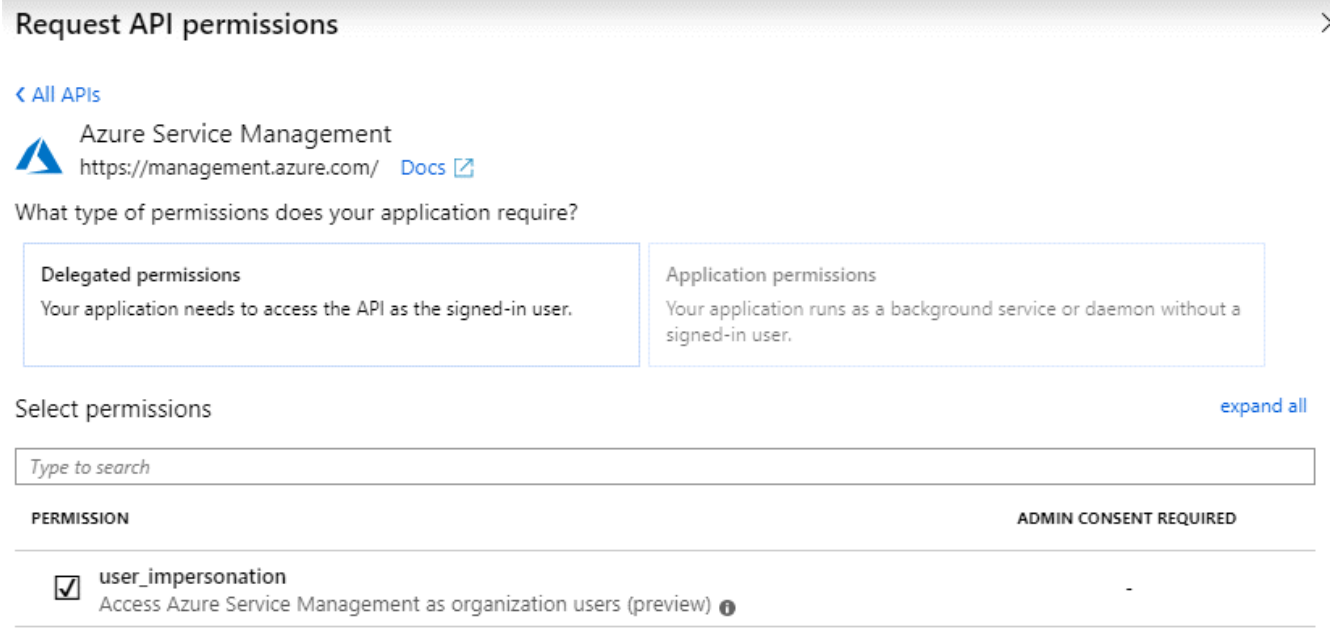
El principal de servicio debe tener permisos de "API de administración de servicios de Windows Azure".

Pasos

1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Seleccione **permisos de API > Agregar un permiso**.
3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.



4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.

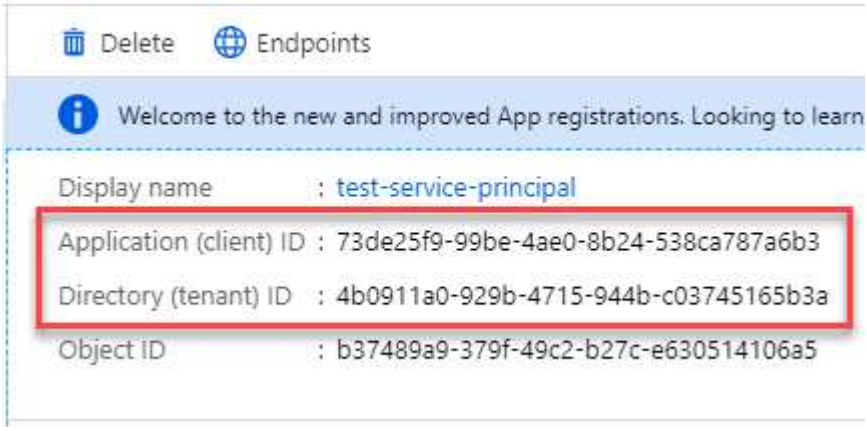


Obtener el ID de aplicación y el ID de directorio

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 **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Cree un secreto de cliente

Debes crear un secreto de cliente y proporcionar a BlueXP el valor del secreto para que BlueXP pueda usarlo para autenticarse con Microsoft Entra ID.

Pasos

1. Abra el servicio **Microsoft Entra ID**.
2. Seleccione **App registres** y seleccione su aplicación.
3. Seleccione **certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copie el valor del secreto de cliente.

Ahora tienes un secreto de cliente que BlueXP puede usarlo para autenticar con Microsoft Entra ID.

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.

Agregue 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.

Antes de empezar

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, seleccione el icono Configuración y seleccione **credenciales**.

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.
   b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:

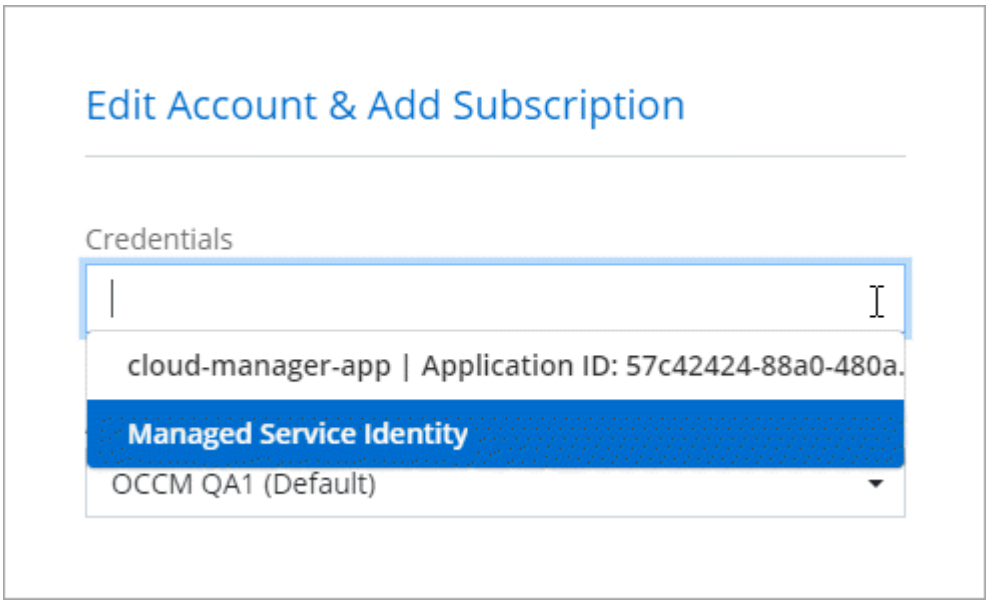
    - ID de aplicación (cliente)
    - ID de directorio (inquilino)
    - Secreto de cliente

c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **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.

Asocie 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 permite crear un sistema Cloud Volumes ONTAP de pago por uso y utilizar otros servicios BlueXP.

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 cambiar la suscripción de Azure Marketplace asociada con las credenciales de Azure.

  La sustitución de la suscripción actual del mercado por una nueva suscripción cambia la suscripción del mercado para cualquier entorno de trabajo existente de Cloud Volumes ONTAP y todos los nuevos entornos de trabajo.

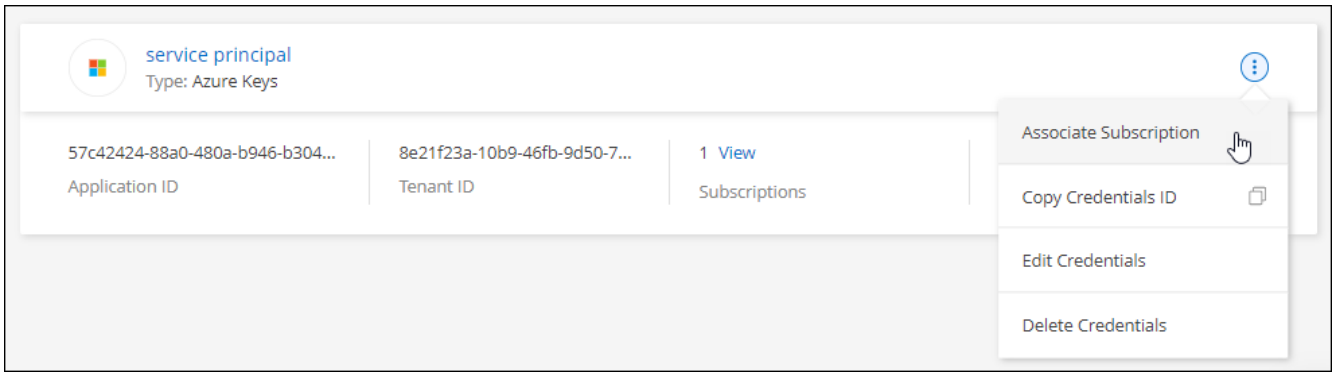
Antes de empezar

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, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y seleccione **asociado**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos de Azure Marketplace:

   a. Si se le solicita, inicie sesión en su cuenta de Azure.

   b. Seleccione **Suscribirse**.

   c. Rellene el formulario y seleccione **Suscribirse**.

   d. Una vez completado el proceso de suscripción, seleccione **Configurar cuenta ahora**.

      Se le redirigirá al sitio web de BlueXP.

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

      - Seleccione las cuentas de BlueXP con 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.

      - Seleccione **Guardar**.

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

   Suscríbete a BlueXP desde Azure Marketplace

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, seleccione el icono Configuración y seleccione **credenciales**.
2. En la página **credenciales de cuenta**, seleccione el menú de acción para un conjunto de credenciales y, a continuación, seleccione **Editar credenciales**.
3. Realice los cambios necesarios y, a continuación, seleccione **aplicar**.

Eliminar 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, seleccione el icono Configuración y seleccione **credenciales**.
2. En la página **credenciales de cuenta**, seleccione el menú de acción para un conjunto de credenciales y, a continuación, seleccione **Eliminar credenciales**.
3. Seleccione **Eliminar** para confirmar.

Google Cloud

Obtén más información sobre los proyectos y permisos de Google Cloud

Descubre cómo BlueXP utiliza las credenciales de Google Cloud para realizar acciones en tu nombre y cómo esas credenciales están asociadas a las suscripciones del mercado. Comprender estos detalles puede resultar útil al administrar las credenciales de uno o más proyectos de Google Cloud. Por ejemplo, es posible que desee obtener información sobre la cuenta de servicio asociada a la VM de Connector.

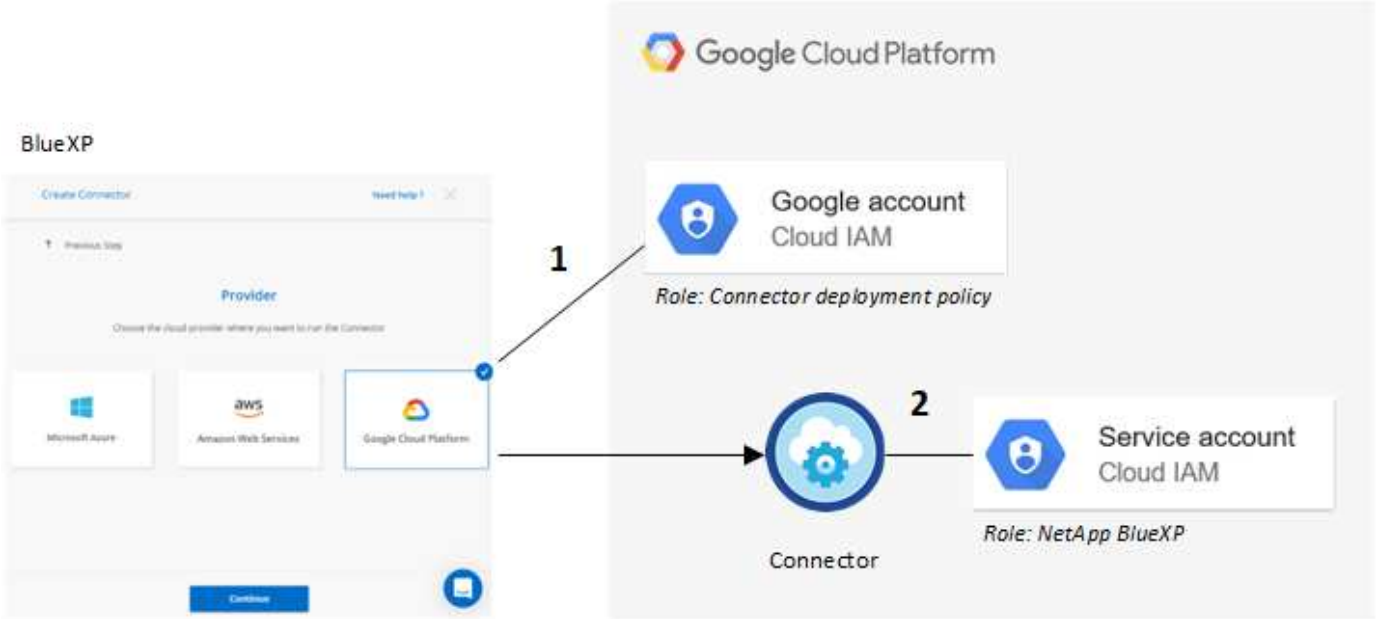
Proyecto y permisos para BlueXP

Antes de poder usar BlueXP para administrar recursos en su proyecto de Google Cloud, primero debe implementar un conector. 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 gestionar sistemas de Cloud Volumes ONTAP, para gestionar backups mediante el backup y la recuperación de BlueXP, y mucho más. Los permisos se proporcionan asociando una función personalizada a la cuenta de servicio.

La siguiente imagen muestra los requisitos de permisos descritos en los números 1 y 2 anteriores:



Para aprender a configurar los permisos, consulte las siguientes páginas:

- "Configure los permisos de Google Cloud para el modo estándar"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

Credenciales y suscripciones de Marketplace

Cuando implementas un Connector en Google Cloud, BlueXP crea un conjunto de credenciales predeterminado para la cuenta de servicio de Google Cloud en el proyecto en el que reside Connector. Estas credenciales deben estar asociadas a una suscripción a Google Cloud Marketplace para poder pagar por Cloud Volumes ONTAP con una tarifa por hora (PAYGO) y utilizar otros servicios de BlueXP.

"Descubre cómo asociar una suscripción a Google Cloud Marketplace".

Tenga en cuenta lo siguiente acerca de las credenciales de Google Cloud y las suscripciones al mercado:

- Solo se puede asociar un conjunto de credenciales de Google Cloud a un conector
- Solo puedes asociar una suscripción a Google Cloud Marketplace a las credenciales
- Puede reemplazar una suscripción existente de Marketplace por una nueva

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 la cuenta de servicio"
- "Descubra cómo implementar Cloud Volumes ONTAP en Google Cloud y seleccione un proyecto"

Administrar las credenciales y suscripciones de Google Cloud para BlueXP

Puede administrar las credenciales de Google Cloud asociadas a la instancia de VM

Connector asociando una suscripción a Marketplace y solucionando el proceso de suscripción. Ambas tareas garantizan que puedas usar tu suscripción al mercado para pagar los servicios de BlueXP.

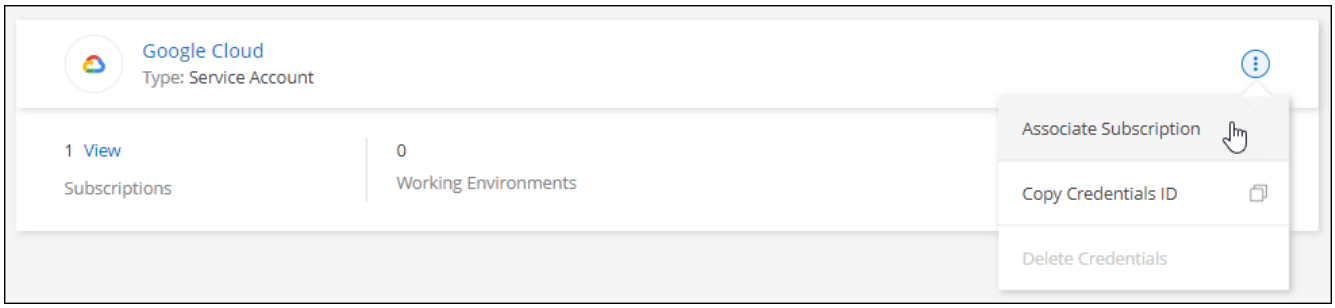
Asocie una suscripción a Marketplace con credenciales de Google Cloud

Al implementar un conector en Google Cloud, BlueXP crea un conjunto predeterminado de credenciales asociadas a la instancia de Connector VM. En cualquier momento, puedes cambiar la suscripción de Google Cloud Marketplace asociada a estas credenciales. La suscripción permite crear un sistema Cloud Volumes ONTAP de pago por uso y utilizar otros servicios BlueXP.

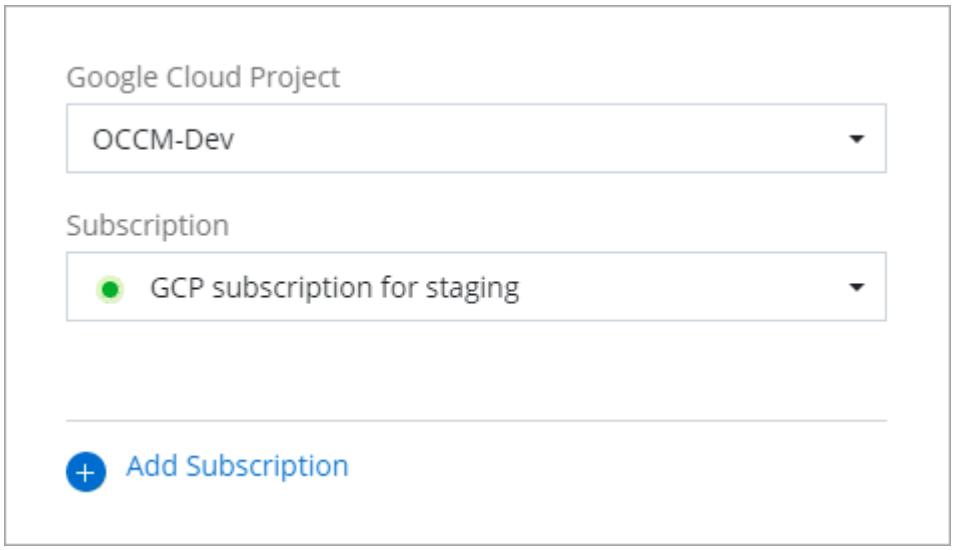
La sustitución de la suscripción actual del mercado por una nueva suscripción cambia la suscripción del mercado para cualquier entorno de trabajo existente de Cloud Volumes ONTAP y todos los nuevos entornos de trabajo.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.



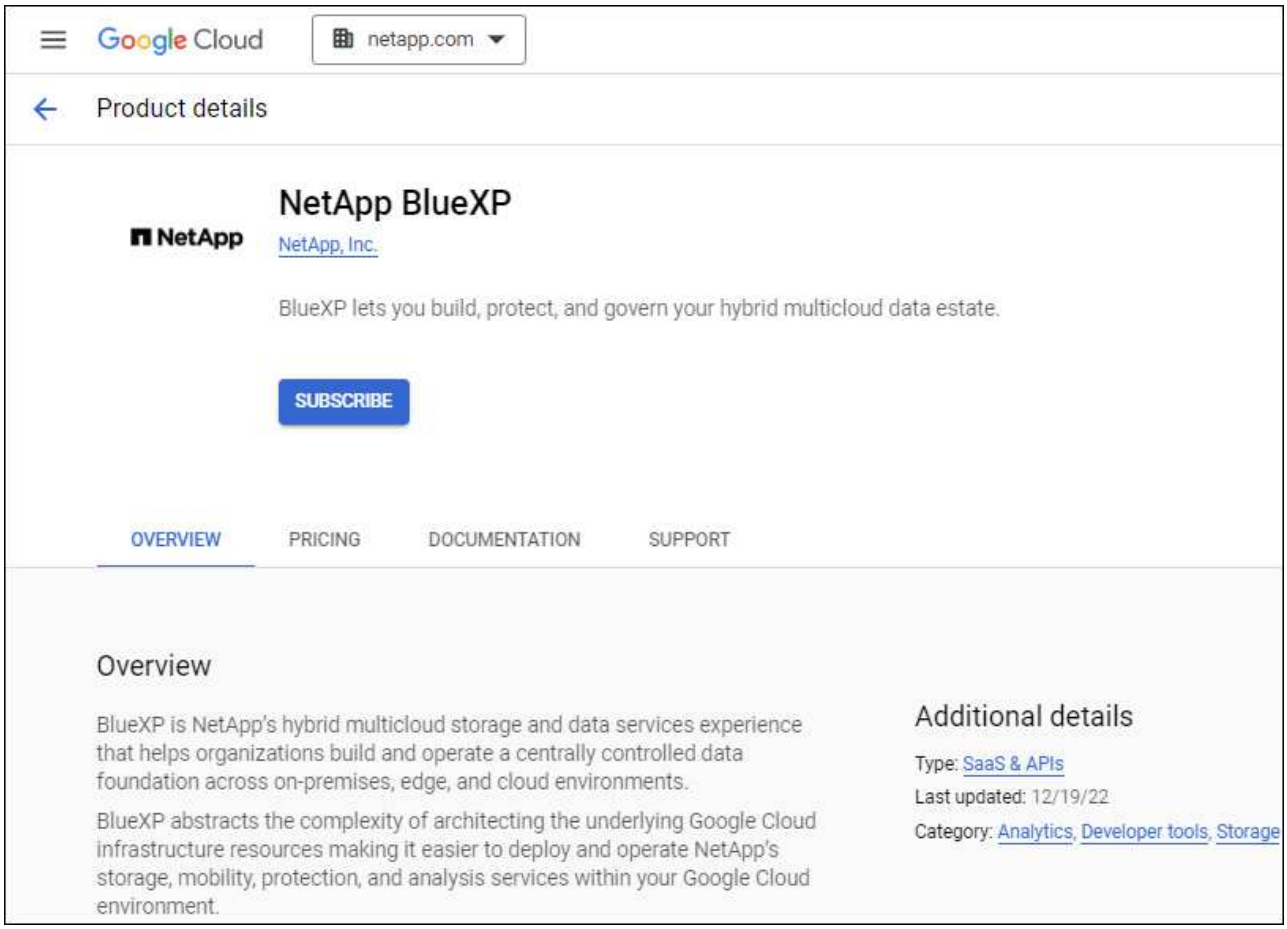
3. Para asociar las credenciales a una suscripción existente, seleccione un proyecto de Google Cloud y una suscripción en la lista desplegable y, a continuación, seleccione **asociado**.



4. Si aún no tiene una suscripción, seleccione **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.



b. Seleccione **Suscribirse**.

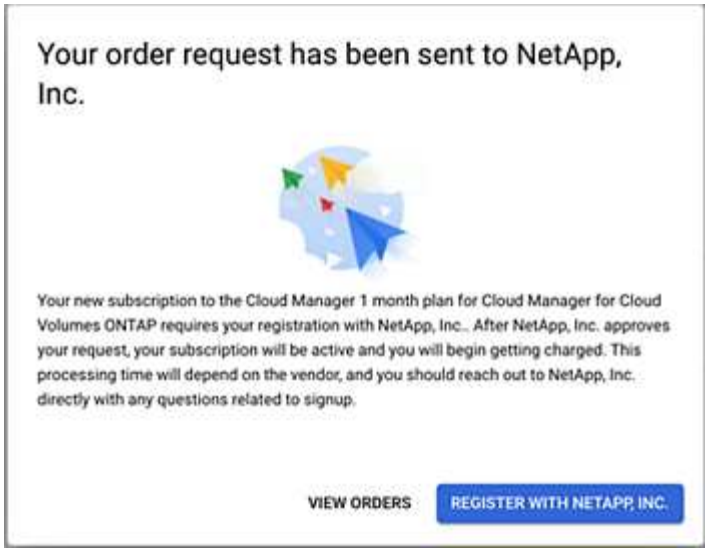
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.

d. Seleccione **Suscribirse**.

   Este paso envía la solicitud de transferencia a NetApp.

e. En el cuadro de diálogo emergente, seleccione **Registro con NetApp, Inc.**

   Este paso debe completarse para vincular la suscripción a Google Cloud a su cuenta de BlueXP. 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 BlueXP con 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.

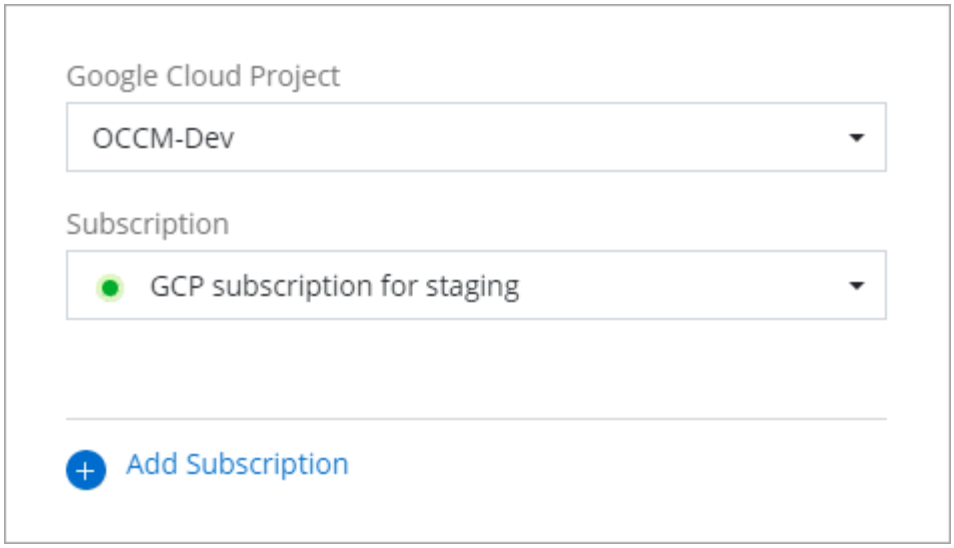
Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

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

Suscríbete a BlueXP desde Google Cloud Marketplace

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

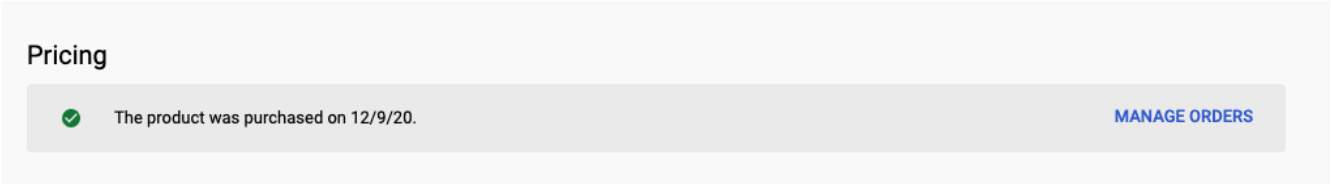


Solucione los problemas del proceso de suscripción a Marketplace

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

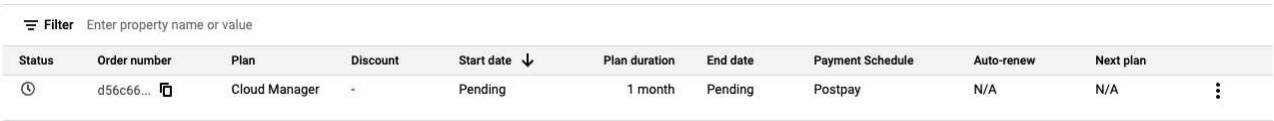
Pasos

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 seleccione **gestionar pedidos**.



   - 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.

   - 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.



Administrar las credenciales de NSS asociadas con una cuenta de BlueXP

Asocie una cuenta del sitio de soporte de NetApp con su cuenta de BlueXP para habilitar los flujos de trabajo clave para Cloud Volumes ONTAP. Estas credenciales de NSS están asociadas a toda la cuenta de BlueXP.

> BlueXP también admite la asociación de una cuenta NSS por usuario de BlueXP. "Aprenda a gestionar las credenciales en el nivel de usuario".

Descripción general

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

- Puesta en marcha de Cloud Volumes ONTAP cuando usted traiga su propia licencia (BYOL)

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

- Registro de sistemas Cloud Volumes ONTAP de pago por uso

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

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

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

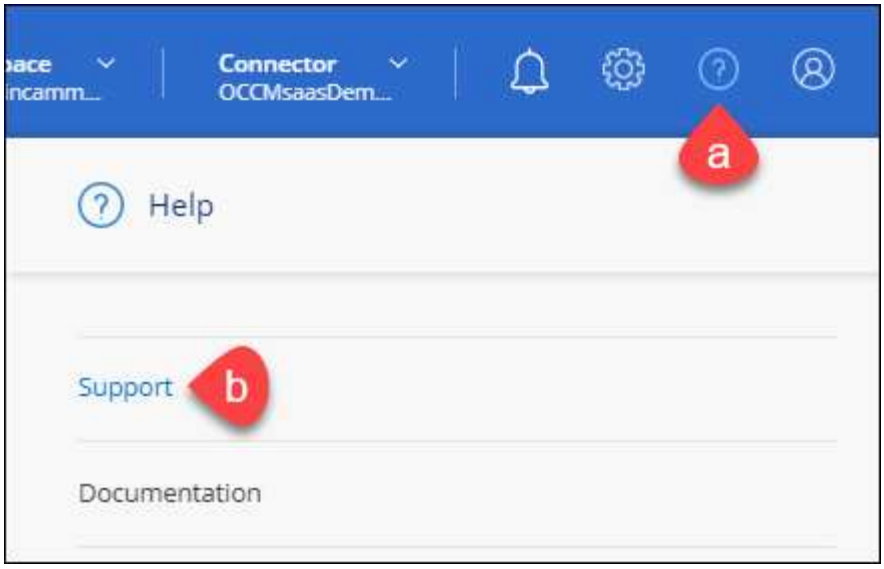
Añada una cuenta de NSS

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

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

Pasos

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



2. Seleccione **Administración de NSS > Agregar cuenta de NSS**.
3. Cuando se le solicite, seleccione **continuar** para que se le redirija a una página de inicio de sesión de Microsoft.

   NetApp utiliza Microsoft Entra ID como proveedor de identidad para los servicios de autenticación específicos de soporte y licencias.

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

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

   Tenga en cuenta lo siguiente:

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

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

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

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

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

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

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

El futuro

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

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

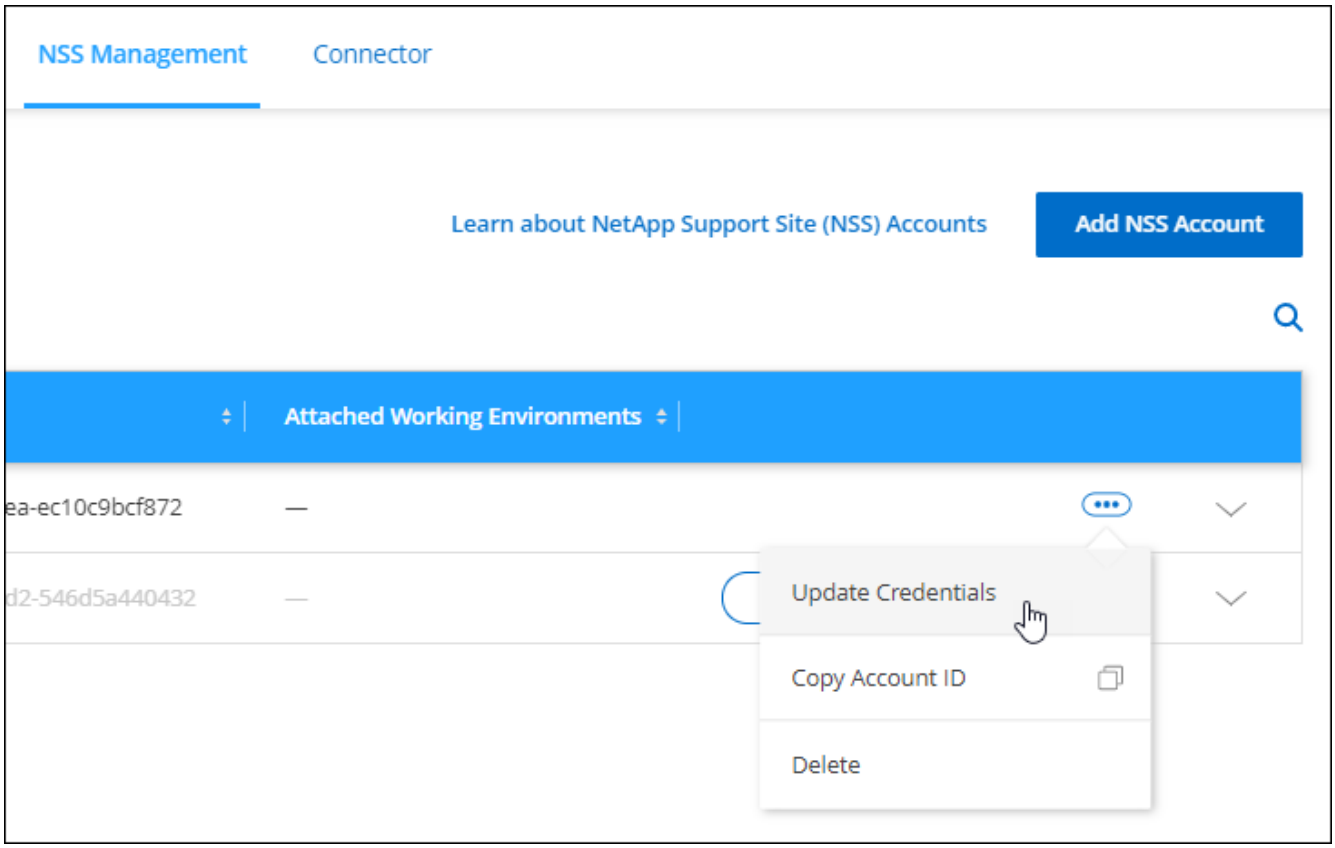
Actualice las credenciales de NSS

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, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **NSS Management**.
3. Para la cuenta de NSS que desea actualizar, seleccione ••• Y, a continuación, seleccione **Actualizar credenciales**.



4. Cuando se le solicite, seleccione **continuar** para que se le redirija a una página de inicio de sesión de Microsoft.

NetApp utiliza Microsoft Entra ID como proveedor de identidad para los servicios de autenticación específicos de 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.

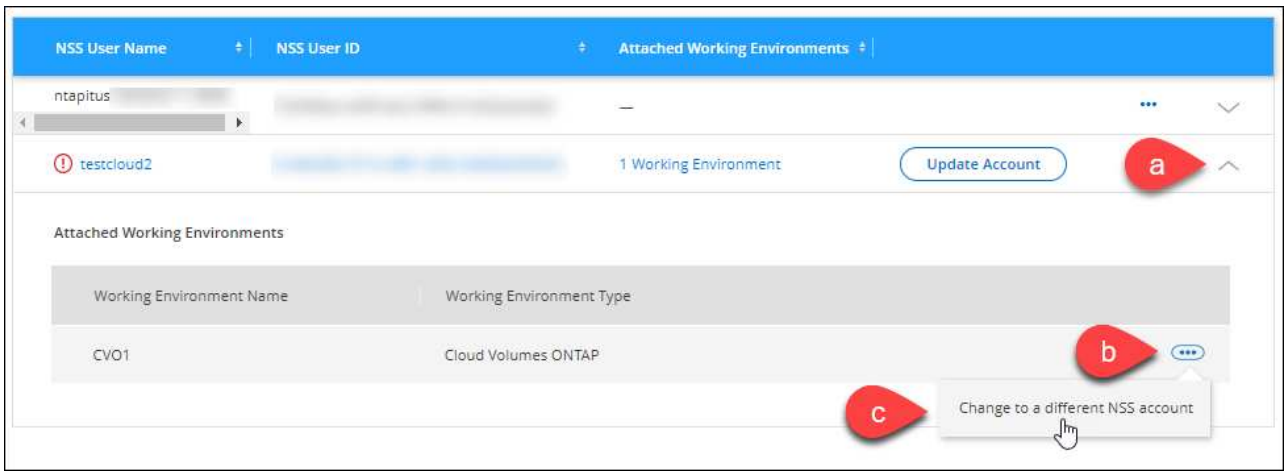
Adjunte un entorno de trabajo a una cuenta de NSS diferente

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 sólo es compatible con cuentas NSS configuradas para utilizar Microsoft Entra ID adoptado por NetApp para la gestión de identidades. Para poder utilizar esta función, necesita seleccionar **Agregar cuenta de NSS** o **Actualizar cuenta**.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **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, seleccione •••
   c. Seleccione **Cambiar a una cuenta de NSS diferente**.



   d. Seleccione la cuenta y, a continuación, seleccione **Guardar**.

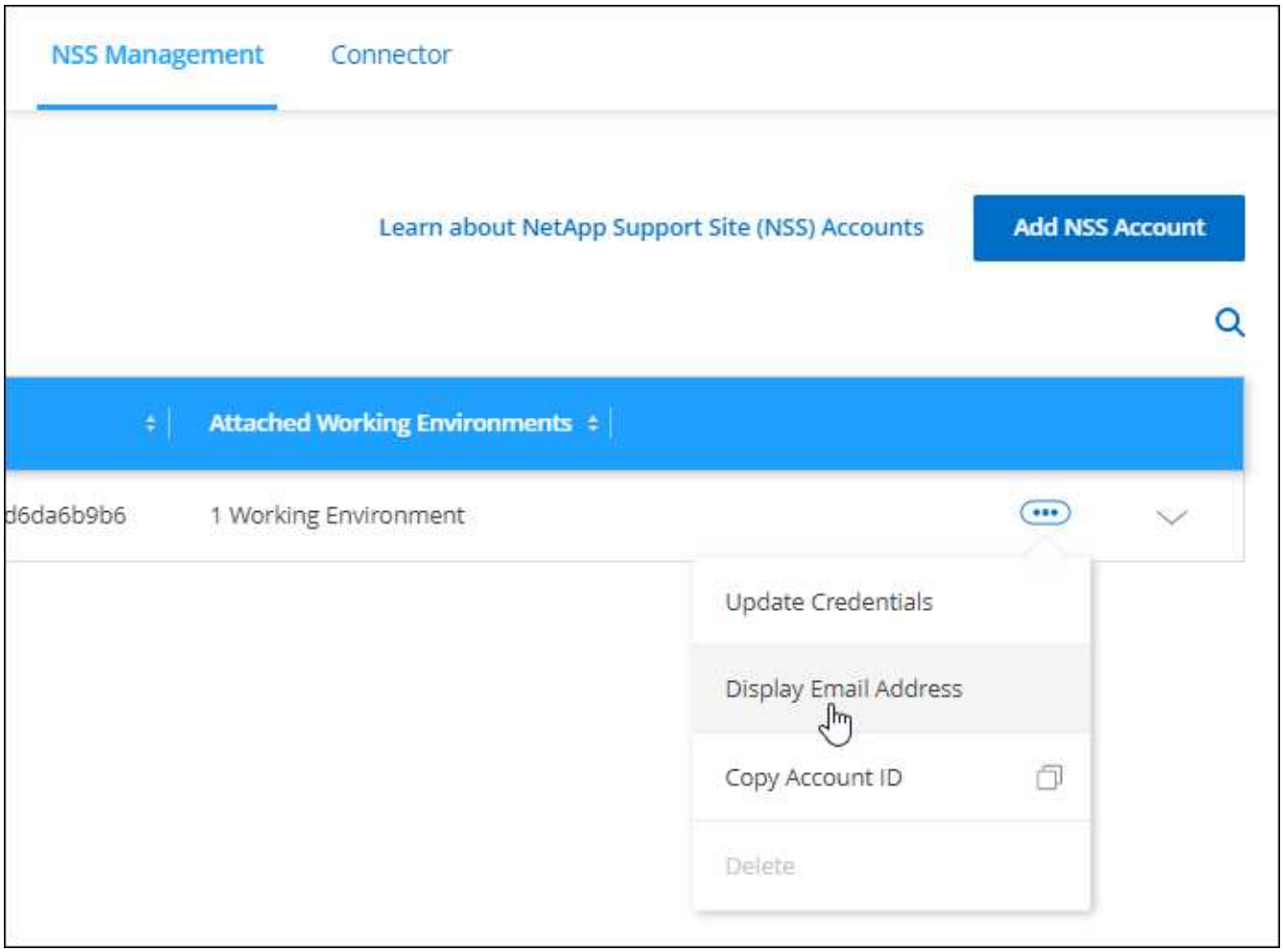
Muestra la dirección de correo electrónico de una cuenta de NSS

Ahora que las cuentas del sitio de soporte de NetApp usan Microsoft Entra ID para los servicios de autenticación, el nombre de usuario NSS que aparece en BlueXP suele ser un identificador generado por Microsoft Entra. 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, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **NSS Management**.
3. Para la cuenta de NSS que desea actualizar, seleccione ••• 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.

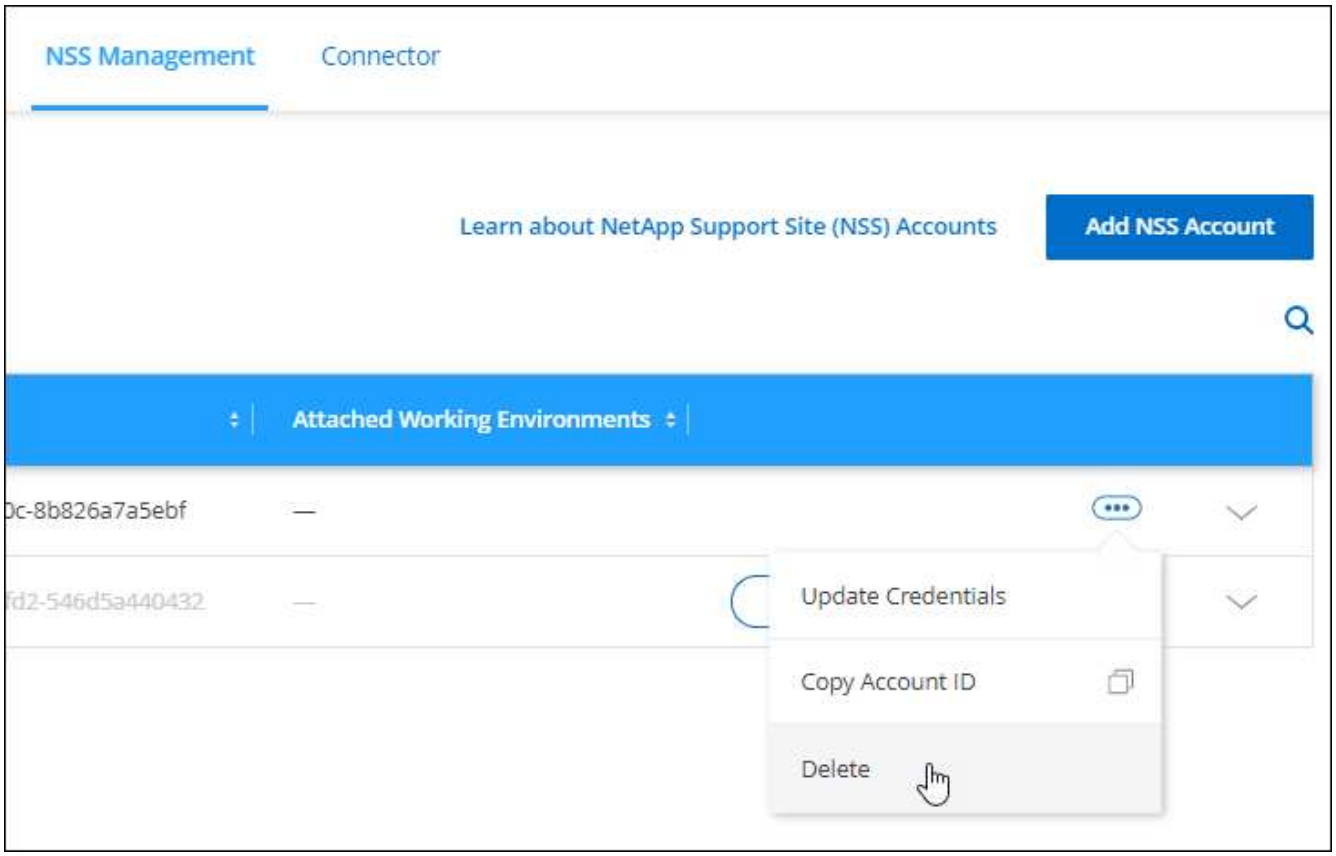
Quite una cuenta de NSS

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, seleccione el icono Ayuda y seleccione **Soporte**.
2. Seleccione **NSS Management**.
3. Para la cuenta de NSS que desea eliminar, seleccione ••• Y, a continuación, seleccione **Eliminar**.



4. Seleccione **Eliminar** para confirmar.

Administre las credenciales asociadas con su inicio de sesión de BlueXP

En función de las acciones que haya adoptado en BlueXP, quizás tenga credenciales de ONTAP asociadas y credenciales del sitio de soporte de NetApp (NSS) con su inicio de sesión de usuario de BlueXP. Puede ver y administrar esas credenciales en BlueXP después de haberlas asociado. Por ejemplo, si cambia la contraseña para estas credenciales, deberá actualizar la contraseña en BlueXP.

Credenciales de ONTAP

Cuando detecta directamente un clúster de ONTAP en las instalaciones sin usar un conector, se le solicita que introduzca las credenciales de ONTAP para el clúster. Estas credenciales se gestionan en el nivel de usuario, lo que significa que otros usuarios que inician sesión no las pueden ver.

Credenciales de NSS

Las credenciales de NSS asociadas con tu inicio de sesión de BlueXP permiten el registro de soporte, la gestión de casos y el acceso al asesor digital.

- Cuando accedes a **Soporte > Recursos** y te registras para recibir soporte, se te pedirá que asocies las credenciales de NSS con tu inicio de sesión de BlueXP.

  Esta acción registra la cuenta de BlueXP para recibir soporte y activa la autorización de soporte. Solo un usuario en tu cuenta de BlueXP debe asociar una cuenta del sitio de soporte de NetApp con su inicio de sesión de BlueXP para registrarse en el servicio de soporte y activar la autorización de soporte. Una vez

completado, la página **Recursos** muestra que su cuenta está registrada para soporte.

"Aprenda a registrarse para obtener soporte"

- Al acceder a **Soporte > Administración de casos**, se le pedirá que introduzca sus credenciales de NSS, si aún no lo ha hecho. Esta página permite crear y gestionar los casos de soporte asociados con su cuenta de NSS y su empresa.
- Al acceder a Digital Advisor en BlueXP, se le pedirá que inicie sesión en Digital Advisor introduciendo sus credenciales de NSS.

Tenga en cuenta lo siguiente sobre la cuenta de NSS asociada con su inicio de sesión de BlueXP:

- La cuenta se gestiona en el nivel de usuario, lo que significa que otros usuarios que inician sesión no la pueden ver.
- Solo puede haber una cuenta de NSS asociada con Digital Advisor y la gestión de casos de soporte, por usuario.
- Si intenta asociar una cuenta del sitio de soporte de NetApp a un entorno de trabajo de Cloud Volumes ONTAP, solo podrá elegir entre las cuentas de NSS que se hayan agregado a la cuenta de BlueXP de la que sea miembro.

  Las credenciales en el nivel de cuenta de NSS son diferentes de la cuenta de NSS asociada con tu inicio de sesión en BlueXP. Las credenciales a nivel de cuenta de NSS le permiten implementar Cloud Volumes ONTAP cuando tiene su propia licencia (BYOL), registrar sistemas PAYGO y actualizar el software Cloud Volumes ONTAP.

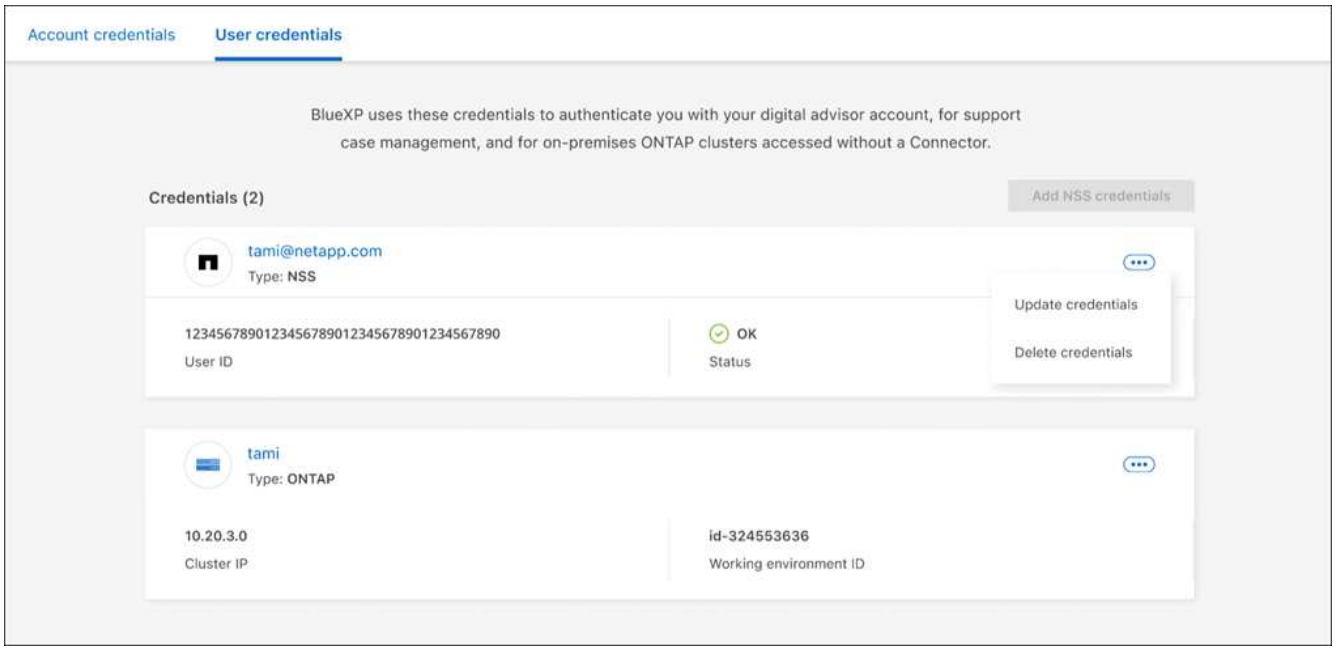
  "Obtenga más información sobre el uso de credenciales de NSS con su cuenta de BlueXP".

Gestione las credenciales de usuario

Para gestionar las credenciales de usuario, actualice el nombre de usuario y la contraseña o elimine las credenciales.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione **Credenciales de usuario**.
3. Si aún no tiene ninguna cuenta de usuario, puede seleccionar **Añadir credenciales de NSS** para añadir su cuenta del sitio de soporte de NetApp.
4. Gestione las credenciales existentes eligiendo las siguientes opciones:
   - **Actualizar credenciales**: Actualizar el nombre de usuario y la contraseña de la cuenta.
   - **Eliminar credenciales**: Elimina la cuenta asociada a tu cuenta de usuario de BlueXP.



Resultado

BlueXP actualiza tus credenciales. Los cambios se reflejarán cuando acceda al clúster de ONTAP, al asesor digital o a la página Gestión de casos.

Referencia

Permisos

Resumen de permisos para BlueXP

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

Permisos de AWS

BlueXP requiere permisos de AWS para el Connector y para servicios individuales.

Conectores

Objetivo	Descripción	Enlace
Pon en marcha el conector de BlueXP	El usuario que crea un conector a partir de BlueXP necesita permisos específicos para implementar la instancia en AWS.	"Configure los permisos de AWS"
Proporcione permisos para el 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. Debe configurar la política usted mismo si inicia un conector desde AWS Marketplace, si instala manualmente el conector o si lo hace "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"

Backup y recuperación

Objetivo	Descripción	Enlace
Realice un backup de los clústeres de ONTAP en las instalaciones en Amazon S3	Al activar backups en tus volúmenes de ONTAP, el backup y recuperación de BlueXP te solicita que introduzcas una clave de acceso y un secreto para un usuario de IAM que tenga permisos específicos.	"Configure los permisos S3 para backups"

Cloud Volumes ONTAP

Objetivo	Descripción	Enlace
Proporcione permisos para los nodos 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 permitir que BlueXP cree los roles de IAM por ti, pero puedes utilizar los tuyos a la hora de crear el entorno de trabajo.	"Aprenda a configurar las funciones del IAM usted mismo"

Copiar y sincronizar

Objetivo	Descripción	Enlace
Ponga en marcha el agente de datos en AWS	La cuenta de usuario de AWS que utilice para implementar el agente de datos debe tener permisos específicos.	"Permisos necesarios para implementar el agente de datos en AWS"
Proporcione permisos para el agente de datos	Cuando la copia y sincronización de BlueXP implementa el agente de datos, crea un rol de IAM para la instancia de agente de datos. Si lo prefiere, puede implementar el agente de datos con su propio rol de IAM.	"Requisitos para usar su propio rol de IAM con AWS agente de datos"
Active el acceso de AWS para un agente de datos instalado manualmente	Si usa el agente de datos con una relación de sincronización que incluya un bloque de S3, debe preparar el host Linux para el acceso a AWS. Cuando instale el agente de datos, deberá proporcionar claves de AWS para un usuario de IAM que tenga acceso programático y permisos específicos.	"Habilitar el acceso a AWS"

FSX para ONTAP

Objetivo	Descripción	Enlace
Crea y gestiona FSx for ONTAP	Para crear o gestionar un entorno de trabajo de Amazon FSx para NetApp ONTAP, debes añadir credenciales de AWS a BlueXP proporcionando el ARN de un rol de IAM que proporcione a BlueXP los permisos necesarios para crear el entorno de trabajo.	"Descubre cómo configurar las credenciales de AWS para FSx"

Organización en niveles

Objetivo	Descripción	Enlace
Organiza clústeres de ONTAP locales en niveles en Amazon S3	Al habilitar la organización en niveles de BlueXP en AWS, el asistente le solicita que introduzca una clave de acceso y una clave secreta. Estas credenciales se pasan al clúster de ONTAP para que ONTAP pueda organizar los datos en niveles en el bloque de S3.	"Configura permisos S3 para la organización en niveles"

Permisos de Azure

BlueXP requiere permisos de Azure para Connector y para servicios individuales.

Conectores

Objetivo	Descripción	Enlace
Pon en marcha el conector de BlueXP	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.	"Configure los permisos de Azure"
Proporcione permisos para el conector	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. Debe configurar el rol personalizado usted mismo si inicia un conector desde el mercado, si instala manualmente el conector o si lo hace "Agregue más credenciales de Azure a un conector". También debe asegurarse de que la directiva esté actualizada a medida que se añadan nuevos permisos en versiones posteriores.	"Permisos de Azure para Connector"

Copiar y sincronizar

Objetivo	Descripción	Enlace
Ponga en marcha el agente de datos en Azure	La cuenta de usuario de Azure que utilice para implementar el agente de datos debe tener los permisos necesarios.	"Permisos necesarios para implementar el agente de datos en Azure"

Permisos de Google Cloud

BlueXP requiere permisos de Google Cloud para Connector y para servicios individuales.

Conectores

Objetivo	Descripción	Enlace
Pon en marcha el conector de BlueXP	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 crear el conector"
Proporcione permisos para el 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 durante el despliegue. También debe asegurarse de que la directiva esté actualizada a medida que se añadan nuevos permisos en versiones posteriores.	"Configure los permisos para el conector"

Backup y recuperación

Objetivo	Descripción	Enlace
Realice backups de Cloud Volumes ONTAP en Google Cloud	Al utilizar el backup y la recuperación de datos de BlueXP para realizar backups de Cloud Volumes ONTAP, debe añadir permisos al conector en las siguientes situaciones: • Desea utilizar la función de búsqueda y restauración • Desea utilizar claves de cifrado gestionadas por el cliente (CMEK)	• "Permisos para la función de Restaurar" • "Permisos para CMEKs"
Realice un backup de los clústeres de ONTAP en las instalaciones en Google Cloud	Al utilizar el backup y la recuperación de datos de BlueXP para realizar backups de clústeres de ONTAP on-premises, tienes que añadir permisos al conector para poder utilizar la funcionalidad de búsqueda y restauración.	"Permisos para la función de Restaurar"

Cloud Volumes Service para Google Cloud

Objetivo	Descripción	Enlace
Descubra Cloud Volumes Service para Google Cloud	BlueXP necesita acceso a la API de Cloud Volumes Service y los permisos adecuados a través de una cuenta de servicio de Google Cloud.	"Configure una cuenta de servicio"

Copiar y sincronizar

Objetivo	Descripción	Enlace
Ponga en marcha el agente de datos en Google Cloud	Asegúrese de que el usuario de Google Cloud que implementa el agente de datos tenga los permisos necesarios.	"Permisos necesarios para implementar el agente de datos en Google Cloud"
Habilita el acceso a Google Cloud para un agente de datos instalado manualmente	Si tiene pensado utilizar el agente de datos con una relación de sincronización que incluya un bucket de Google Cloud Storage, debería preparar el host Linux para el acceso a Google Cloud. Al instalar el Data Broker, deberá proporcionar una clave para una cuenta de servicio que tenga permisos específicos.	"Habilitar el acceso a Google Cloud"

Permisos de StorageGRID

BlueXP requiere permisos de StorageGRID para dos servicios.

Backup y recuperación

Objetivo	Descripción	Enlace
Realice un backup de los clústeres de ONTAP en las instalaciones en StorageGRID	Cuando preparas StorageGRID como destino de backup para los clústeres de ONTAP, el backup y la recuperación de BlueXP le solicita que introduzca una clave de acceso y un secreto para un usuario de IAM que tiene permisos específicos.	"Preparar StorageGRID como destino de backup"

Organización en niveles

Objetivo	Descripción	Enlace
Organiza clústeres de ONTAP on-premises en StorageGRID	Cuando configuras la organización en niveles de BlueXP en StorageGRID, tienes que proporcionar la organización en niveles de BlueXP con una clave de acceso S3 y una clave secreta. La organización en niveles de BlueXP utiliza las claves para acceder a tus buckets.	"Prepare la organización en niveles en StorageGRID"

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.

Tenga en cuenta lo siguiente:

- 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.
- Debe configurar las políticas usted mismo si pone en marcha el conector desde AWS Marketplace, si instala manualmente el conector en un host Linux o si desea añadir credenciales de AWS adicionales a BlueXP.
- También debe asegurarse de que las directivas estén actualizadas a medida que se añadan nuevos permisos en versiones posteriores.
- Si es necesario, puede restringir las políticas de IAM mediante el IAM `Condition` elemento. "Documentación de AWS: Elemento de condición"
- Para ver instrucciones paso a paso para utilizar estas directivas, consulte las páginas siguientes:
  - "Configure los permisos para una puesta en marcha de AWS Marketplace"
  - "Configure los permisos para implementaciones en las instalaciones"
  - "Configure los permisos para el modo restringido"
  - "Configurar permisos para el modo privado"

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:

- Detección de bloques de Amazon S3
- Backup y recuperación
- Clasificación
- Cloud Volumes ONTAP
- FSX para ONTAP
- Organización en niveles

La segunda directiva proporciona permisos para los siguientes servicios:

- Almacenamiento en caché en el edge
- Kubernetes

Política #1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "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",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "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: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

```
{
    "Version": "2012-10-17",
    "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"
        }
    ]
}
```

Regiones GovCloud (EE. UU.

```
{
    "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",
                "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/*"
            ]
        }
    ]
}
```

Regiones secretas

```
{
    "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-b: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-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Regiones Top Secret

```
{
    "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 BlueXP. Esta información puede ser útil si sus políticas corporativas dictan que los permisos sólo se proporcionan según sea necesario.

Amazon FSX para ONTAP

El conector realiza las siguientes solicitudes de API para administrar Amazon FSx for ONTAP:

- ec2:DescribInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkinterfaces
- ec2:DescribeSubnets

- ec2:DescribeVpcs
- ec2:DescribDhcpOptions
- ec2:DescribSnapshots
- ec2:DescribeKeyPairs
- ec2:regiones describidas
- ec2:etiquetas a describTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribVolumesModificaciones
- ec2:DescribePlacementGroups
- Kms:Lista*
- Kms:describir*
- Kms:CreateGrant
- Kms:ListAliases
- fsx:describe*
- fsx:List*

Detección de bloques de Amazon S3

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

s3:GetEncryptionConfiguration

Backup y recuperación

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

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLipeycleConfiguration
- s3:PutBucketEtiquetado
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Kms:Lista*
- Kms:describir*

- 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:PutLipeycleConfiguration
- 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

Clasificación

Connector realiza las siguientes solicitudes de la API para poner en marcha la instancia de clasificación de BlueXP:

- ec2:DescribInstances
- 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 describidas
- Cloudformation:CreateStack
- Cloudformation:DeleteStack
- Cloudformation:Describacks
- Cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

El conector realiza las siguientes solicitudes de la API para analizar los bloques de S3 cuando utilizas la clasificación de BlueXP:

- 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

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:DisasociateIamInstanceProfile	No	Sí	No
Descodificar mensajes de estado de autorización	sts:DecodeAuthorizationMessage	Sí	Sí	No
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

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Detener, iniciar y supervisar instancias	ec2:StartuStarInstances	Sí	Sí	No
	ec2:StopInstances	Sí	Sí	No
	ec2:DescribInstances	Sí	Sí	No
	ec2:DescribeInstanceStatus	Sí	Sí	No
	ec2:RunInstances	Sí	No	No
	ec2:TerminateInstances	No	No	Sí
	ec2:ModificyInstanceAttribute	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
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

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
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:ModificyNetworkInterfaceAttribute	No	Sí	No
Obtenga la lista de subredes de destino y grupos de seguridad	ec2:DescribeSubnets	Sí	Sí	No
	ec2:DescribeVpcs	Sí	Sí	No
Obtenga los servidores DNS y el nombre de dominio predeterminado para las instancias de Cloud Volumes ONTAP	ec2:DescribDhcpOptions	Sí	No	No
Tome snapshots de volúmenes de EBS para Cloud Volumes ONTAP	ec2:CreateSnapshot	Sí	Sí	No
	ec2:DeleteSnapshot	No	Sí	Sí
	ec2:DescribSnapshots	No	Sí	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
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:regiones describidas	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:Describacks	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:PutLipeycleConfiguration	No	Sí	No
	s3:PutBucketEtiquetado	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
	Kms:GenerateDataKeyWithoutPlaintext	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 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:DescribVolumes Modificaciones	No	Sí	No
	ec2:ModifiyVolume	No	Sí	No

Almacenamiento en caché en el edge

Connector realiza las siguientes solicitudes de API para poner en marcha las instancias de almacenamiento en caché perimetral de BlueXP durante la puesta en marcha:

- Cloudformation:Describacks
- Cloudwatch:GetMetricStatistics
- Cloudformation:ListStacks

Kubernetes

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

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

Registro de cambios

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

8 de marzo de 2024

Ahora se incluye el siguiente permiso en la directiva Connector:

EC2:DescripciónAvailabilityZones

Este permiso es necesario para una próxima versión. Actualizaremos las notas de la versión con más detalles cuando esa versión esté disponible.

6 de junio de 2023

Ahora se necesita el siguiente permiso para Cloud Volumes ONTAP:

Kms:GenerateDataKeyWithoutPlaintext

14 de febrero de 2023

Ahora se necesita el siguiente permiso para la organización en niveles de BlueXP:

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.

Para ver instrucciones paso a paso para utilizar estas directivas, consulte las páginas siguientes:

- "Configure los permisos para una puesta en marcha de Azure Marketplace"
- "Configure los permisos para implementaciones en las instalaciones"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

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/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/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/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/acti
on",

"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/acti
on",
```

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

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read"
    ],
    "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 BlueXP. Esta información puede ser útil si sus políticas corporativas dictan que los permisos sólo se proporcionan según sea necesario.

Azure NetApp Files

El conector realiza las siguientes solicitudes de API cuando usas la clasificación de BlueXP para analizar datos 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 y recuperación

El conector realiza las siguientes solicitudes de API para la copia de seguridad y la recuperación de BlueXP:

- 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.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/despliegues/DELETE
- 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

Clasificación

El conector realiza las siguientes solicitudes de la API cuando usas la clasificación de BlueXP.

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/blobServices/contenedores/lectura	Sí	Sí

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
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
Microsoft.Resources/resources/read	Sí	Sí

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

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?
Permite crear y gestionar máquinas virtuales	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
	Microsoft.Compute/virtualMachines/delete	Sí	Sí	Sí
	Microsoft.Resources/despliegues/DELETE	Sí	No	No

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
Habilite la puesta en marcha desde un disco duro virtual	Microsoft.Compute/images/read	Sí	No	No
	Microsoft.Compute/images/write	Sí	No	No
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
	Microsoft.Network/networkInterfaces/delete	Sí	Sí	No
Crear y administrar grupos de seguridad de red	Microsoft.Network/networkSecurityGroups/read	Sí	Sí	No
	Microsoft.Network/networkSecurityGroups/write	Sí	Sí	No
	Microsoft.Network/networkSecurityGroups/join/action	Sí	No	No
	Microsoft.Network/networkSecurityGroups/delete	No	Sí	Sí

Específico	Acción	¿Se utiliza para la puesta en marcha?	¿Se utiliza para operaciones diarias?	¿Se utiliza para su eliminación?
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/leer	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/usos/lectura	No	Sí	No
Permita los backups al almacenamiento BLOB y el cifrado de cuentas de almacenamiento	Microsoft.Storage/storageAccounts/blobServices/contenedores/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.MarketPlaceOrdenar/offertypes/editores/ofertas/planes/acuerdos/leer	Sí	No	No
	Microsoft.MarketPlaceOrdenar/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	No	No
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Sí	No	No
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	Sí	Sí	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
Necesario para algunas implementaciones 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	No
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	No	Sí	No
	Microsoft.Network/networkSecurityGroups/securityRules/write	Sí	Sí	No
	Microsoft.Network/applicationSecurityGroups/delete	No	Sí	Sí
	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

Almacenamiento en caché en el edge

Connector realiza las siguientes solicitudes de API cuando utilizas el almacenamiento en caché perimetral de BlueXP:

- 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

Organización en niveles

El conector realiza las siguientes solicitudes de API al configurar la organización en niveles de BlueXP.

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

El conector realiza las siguientes solicitudes API para operaciones diarias.

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

Registro de cambios

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

5 de diciembre de 2023

Ya no son necesarios los siguientes permisos para el backup y la recuperación de BlueXP al realizar backups de datos de volúmenes en el almacenamiento de Azure Blob:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

Estos permisos son necesarios para otros servicios de almacenamiento de BlueXP, por lo que seguirán teniendo el rol personalizado de Connector si utilizas esos otros servicios de almacenamiento.

12 de mayo de 2023

Se agregaron los siguientes permisos a la política JSON porque son necesarios para la gestión de Cloud Volumes ONTAP:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

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

- Microsoft.Storage/storageAccounts/blobServices/contenedores/escritura
- Microsoft.Network/publicIPAddresses/delete

23 de marzo de 2023

El permiso «Microsoft.Storage/storageAccounts/delete» ya no es necesario para la clasificación de BlueXP.

Este permiso sigue siendo necesario para Cloud Volumes ONTAP.

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

  Se requieren estos permisos para backup y recuperación de BlueXP.

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

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

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.

- "Configure los permisos de Google Cloud para el modo estándar"
- "Configure los permisos para el modo restringido"
- "Configurar permisos para el modo privado"

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.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Para crear reglas de firewall para Cloud Volumes ONTAP.
- Compute.globalOperations.get	Para obtener el estado de las operaciones.

Acciones	Específico
- 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.regions.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
- 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	Para poner en marcha la instancia de máquina virtual de Cloud Volumes ONTAP mediante Google Cloud Deployment Manager.
- Logging.logEntries.list - Logging.privateLogEntries.list	Para obtener unidades de registro de pila.
- resourcemanager.projects.get	Para dar soporte a proyectos múltiples.
- 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.
- cloudkms.cryptoKeyVersions.useToEncrypt - Cloudkms.cryptoKeys.get - Cloudkms.cryptoKeys.list - Cloudkms.keyrings.list	Para utilizar claves de cifrado gestionadas por el cliente desde el Servicio de gestión de claves cloud con Cloud Volumes ONTAP.
- 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.
- Compute.backendServices.create - Compute.regionBackendServices.create - Compute.regionBackendServices.get - Compute.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.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	Para habilitar la clasificación de BlueXP.

Acciones	Específico
- container.clusters.get - container.clusters.list	Para detectar los clústeres de Kubernetes que se ejecutan en Google Kubernetes Engine.
- compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface	Crear y gestionar máquinas virtuales de almacenamiento en pares de alta disponibilidad de Cloud Volumes ONTAP.
- MONITORING.TIMEERIES.LIST - Storage.buckets.getIamPolicy	Para descubrir información sobre cubos de Google Cloud Storage.
- Cloudkms.cryptoKeys.get - Cloudkms.cryptoKeys.getIamPolicy - Cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - Cloudkms.keyrings.get - Cloudkms.keyrings.getIamPolicy - Cloudkms.keyrings.list - cloudkms.keyRings.setIamPolicy	Para seleccionar tus propias claves gestionadas por el cliente en el asistente de activación de backup y recuperación de BlueXP en lugar de usar las claves de cifrado gestionadas por Google predeterminadas.

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

Se requieren estos permisos para backup y recuperación de BlueXP.

Puertos

Reglas de grupo de seguridad de conector en AWS

El grupo de seguridad de AWS para Connector requiere reglas tanto entrantes como salientes. BlueXP crea automáticamente este grupo de seguridad cuando creas un conector desde BlueXP. Debe configurar este grupo de seguridad para todas las demás

opciones de instalación.

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 • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Ofrece acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local y conexiones desde la instancia de clasificación de BlueXP
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 información sobre cómo se utiliza el conector como proxy para los mensajes de AutoSupport"
TCP	9060, 9061	Proporciona la capacidad de habilitar y utilizar la clasificación de BlueXP y el backup y la recuperación de datos de BlueXP en regiones gubernamentales.

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	Llamadas API a AWS, a ONTAP, a la clasificación de BlueXP y al enviar mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	Mediador de alta disponibilidad de ONTAP	Comunicación con el mediador de alta disponibilidad de ONTAP
	TCP	8080	Clasificación de BlueXP	Sondee la instancia de clasificación de BlueXP durante la puesta en marcha
DNS	UDP	53	DNS	Utilizado para resolver DNS por BlueXP

Reglas de grupo de seguridad de conector en Azure

El grupo de seguridad de Azure para Connector requiere reglas tanto entrantes como salientes. BlueXP crea automáticamente este grupo de seguridad cuando creas un conector desde BlueXP. Debe configurar este grupo de seguridad para todas las demás opciones de instalación.

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 • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Ofrece acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local y conexiones desde la instancia de clasificación de BlueXP

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 información sobre cómo se utiliza el conector como proxy para los mensajes de AutoSupport"
TCP	9060, 9061	Proporciona la capacidad de habilitar y utilizar la clasificación de BlueXP y el backup y la recuperación de datos de BlueXP en regiones gubernamentales.

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	Llamadas API a Azure, a ONTAP, a la clasificación de BlueXP y al enviar mensajes de AutoSupport a NetApp
Llamadas API	TCP	8080	Clasificación de BlueXP	Sondee la instancia de clasificación de BlueXP durante la puesta en marcha

Servicio	Protocolo	Puerto	Destino	Específico
DNS	UDP	53	DNS	Utilizado para resolver DNS por BlueXP

Reglas de firewall de conector en Google Cloud

Las reglas de firewall de Google Cloud para el conector requieren reglas tanto entrantes como salientes. BlueXP crea automáticamente este grupo de seguridad cuando creas un conector desde BlueXP. Debe configurar este grupo de seguridad para todas las demás opciones de instalación.

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 • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario
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 información sobre cómo se utiliza el conector como proxy para los mensajes de AutoSupport"

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	Llamadas API a Google Cloud, a ONTAP, a la clasificación de BlueXP y al enviar mensajes de AutoSupport a NetApp
Llamadas API	TCP	8080	Clasificación de BlueXP	Sondee la instancia de clasificación de BlueXP durante la puesta en marcha
DNS	UDP	53	DNS	Utilizado para resolver DNS por BlueXP

Puertos para el conector en las instalaciones

El conector utiliza los puertos *inbound* cuando se instala manualmente en un host Linux local. Es posible que necesite consultar estos puertos para fines de planificación.

Estas reglas de entrada se aplican a todos los modelos de implementación de BlueXP.

Protocolo	Puerto	Específico
HTTP	80	• Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Conocimiento y apoyo

Regístrese para recibir soporte

Es necesario registrarse en soporte para recibir soporte técnico específico para BlueXP y sus servicios y soluciones de almacenamiento. También es necesario registrar soporte para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP.

Al registrarse para recibir soporte, no se habilita el soporte de NetApp para un servicio de archivos de proveedor de cloud. Para obtener soporte técnico relacionado con un servicio de archivos del proveedor de cloud, su infraestructura o cualquier solución que utilice el servicio, consulte «Obtener 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. Para completar el registro, añade cuentas del sitio de soporte de NetApp (NSS) a BlueXP, como se describe a continuación.

Registra tu cuenta de BlueXP para recibir soporte de NetApp

Para registrarte para obtener soporte y activar el soporte, un usuario de tu cuenta de BlueXP debe asociar una cuenta en el sitio de soporte de NetApp a su inicio de sesión en BlueXP. 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

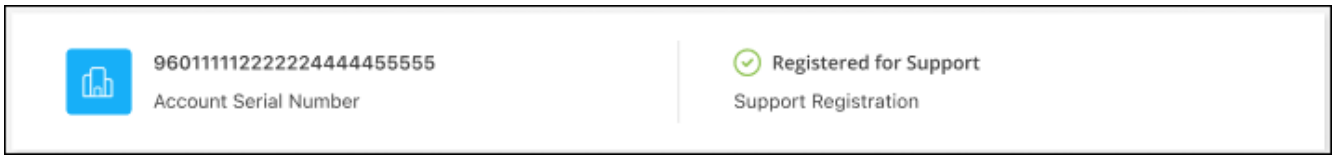
Si es cliente de NetApp con una cuenta de NSS, solo tiene que registrarse para recibir soporte a través de BlueXP.

Pasos

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

2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga el aviso de autenticación del sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro se ha realizado correctamente, seleccione el icono Ayuda y seleccione **Soporte**.

   La página **Recursos** debe mostrar que su cuenta está registrada para soporte.

   Tenga en cuenta que los otros usuarios de BlueXP no verán este mismo estado de registro de soporte si no han asociado una cuenta del sitio de soporte de NetApp con su inicio de sesión de BlueXP. Sin embargo, eso no significa que tu cuenta de BlueXP no esté registrada para el soporte técnico. Siempre y cuando un usuario de la cuenta haya seguido estos pasos, su cuenta se ha registrado.

Cliente existente pero no cuenta NSS

Si eres un cliente existente de NetApp con licencias y números de serie existentes, pero *no* NSS, deberás crear una cuenta NSS y asociarla al inicio de sesión de BlueXP.

Pasos

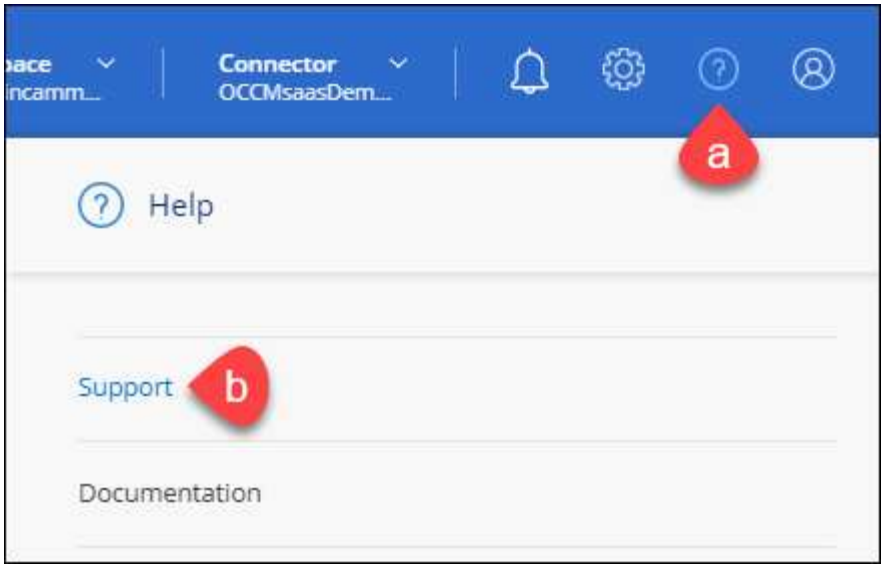
1. Complete el para crear una cuenta en la página de soporte de NetApp "Formulario de registro de usuarios del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario adecuado, que normalmente es **Cliente/Usuario final de NetApp**.
   b. Asegúrese de copiar el número de serie de la cuenta BlueXP (960xxxx) utilizado anteriormente para el campo de número de serie. Esto agilizará el procesamiento de la cuenta.
2. Asocia tu nueva cuenta de NSS con tu inicio de sesión de BlueXP. Para ello, sigue los pasos que se muestran en Cliente existente con una cuenta de NSS.

Totalmente nuevo en NetApp

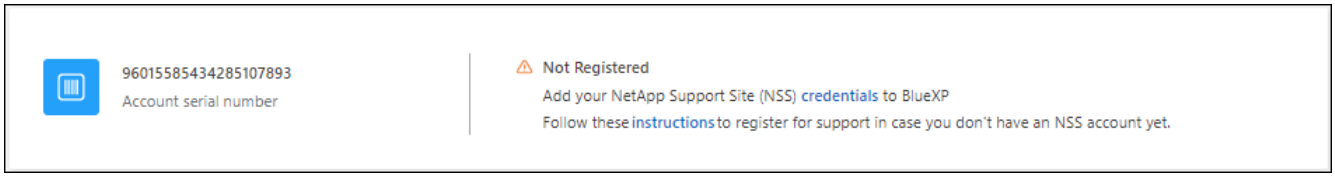
Si es totalmente nuevo en NetApp y no tiene una cuenta de NSS, siga cada paso que se indica a continuación.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione 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.

Cuando tengas tu cuenta en el sitio de soporte de NetApp, asocia la cuenta con el inicio de sesión de BlueXP siguiendo los pasos que se muestran a continuación Cliente existente con una cuenta de NSS.

Asocie credenciales de NSS para soporte de Cloud Volumes ONTAP

Es necesario asociar las credenciales del sitio de soporte de NetApp con su cuenta de BlueXP para habilitar los siguientes flujos de trabajo clave para Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pago por uso para recibir soporte

  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.

- Puesta en marcha de Cloud Volumes ONTAP cuando usted traiga su propia licencia (BYOL)

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

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

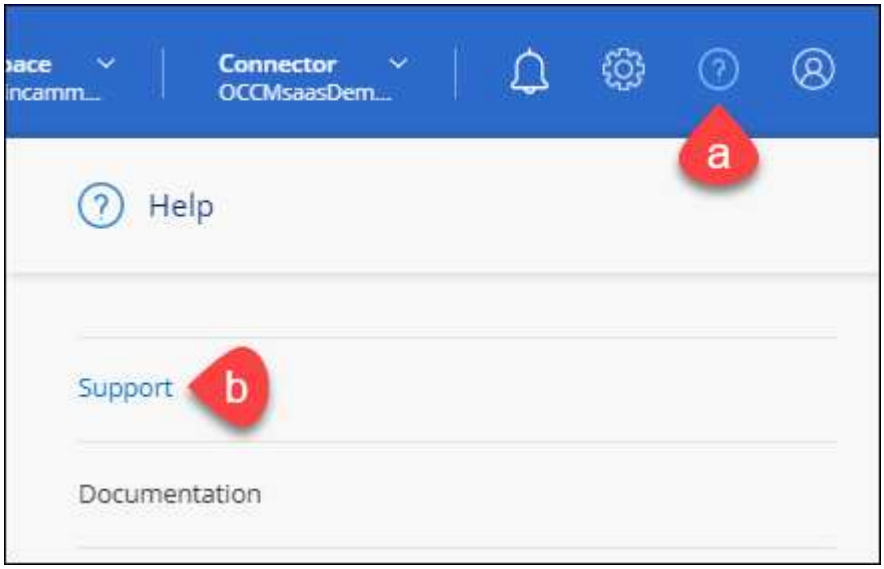
La asociación de credenciales de NSS con su cuenta de BlueXP es diferente de la cuenta de NSS asociada con un inicio de sesión de usuario de BlueXP.

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

- 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, seleccione el icono Ayuda y seleccione **Soporte**.



2. Seleccione **Administración de NSS > Agregar cuenta de NSS**.
3. Cuando se le solicite, seleccione **continuar** para que se le redirija a una página de inicio de sesión de

Microsoft.

NetApp utiliza Microsoft Entra ID como proveedor de identidad para los servicios de autenticación específicos de soporte y licencias.

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

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

   Tenga en cuenta lo siguiente:

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

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

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

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

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

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

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

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.

Obtenga soporte para un servicio de archivos de proveedores de cloud

Para obtener soporte técnico relacionado con un servicio de archivos del proveedor de cloud, su infraestructura o cualquier solución que utilice el servicio, consulte «Obtener ayuda» en la documentación de BlueXP para ese producto.

- "Amazon FSX para ONTAP"
- "Azure NetApp Files"

- "Cloud Volumes Service para Google Cloud"

Para recibir soporte técnico específico sobre BlueXP y sus soluciones y servicios de almacenamiento, use las opciones de soporte descritas a continuación.

Utilice opciones de soporte automático

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

- Documentación

  La documentación de BlueXP que está viendo actualmente.

- "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.

Cree un caso con el 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 funcionalidad **Crear un caso**, primero debes asociar tus credenciales del sitio de soporte de NetApp con el inicio de sesión de BlueXP. "Descubre cómo gestionar las credenciales asociadas con tu inicio de sesión de BlueXP".
- Si abre un caso para un sistema ONTAP que tiene un número de serie, su cuenta de NSS deberá estar asociada con el número de serie de ese sistema.

Pasos

1. En BlueXP, selecciona **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:

   a. Selecciona **Llámanos** si quieres hablar con alguien por teléfono. Se le dirigirá a una página de netapp.com que enumera los números de teléfono a los que puede llamar.

   b. Selecciona **Crear un caso** para abrir un ticket con un especialista en Soporte NetApp:

      - **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.

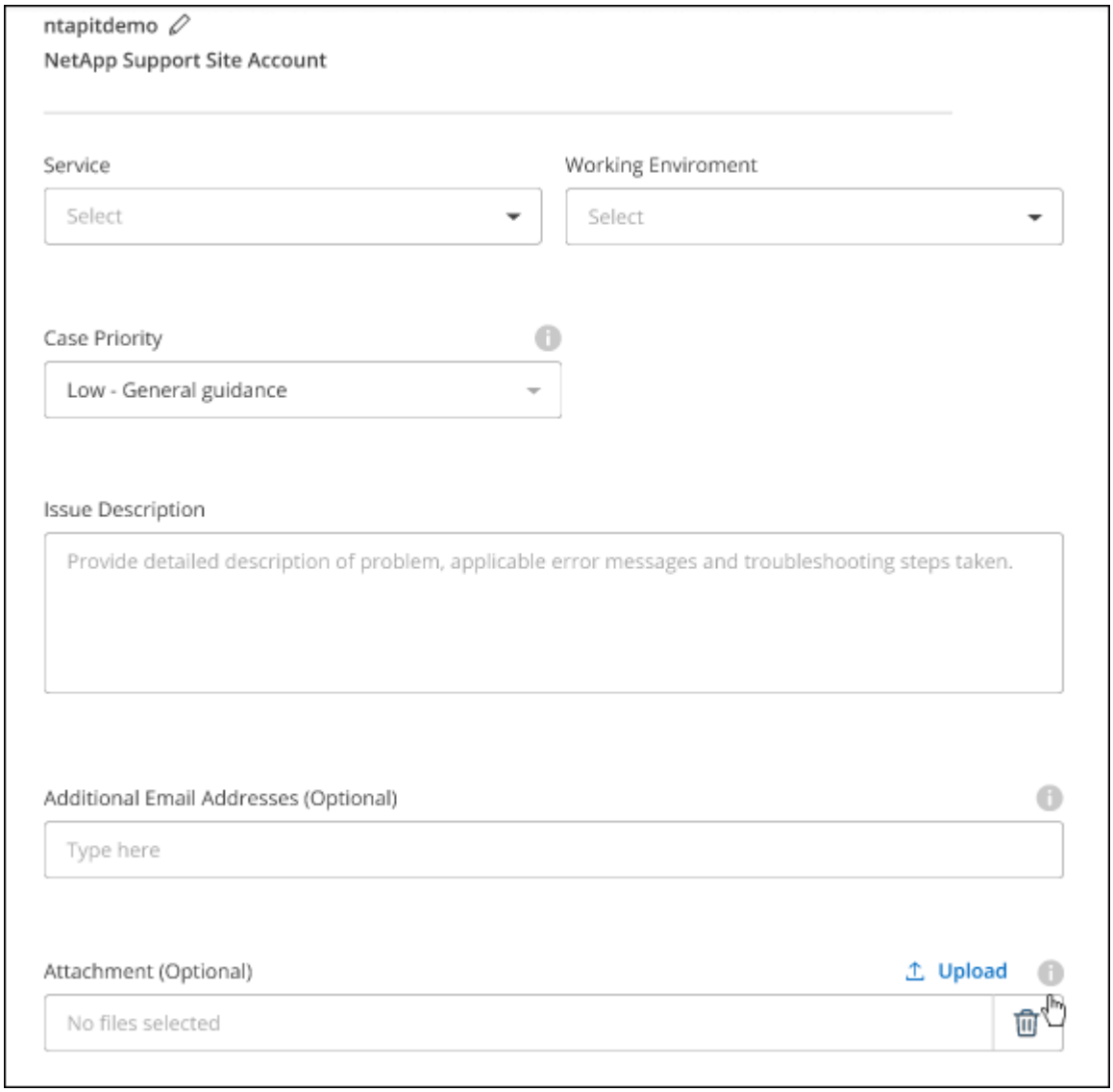
      - **Prioridad de caso**: Elija la prioridad para el caso, que puede ser Baja, Media, Alta o crítica.

        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.
- **Accesorio (opcional)**: Cargue hasta cinco archivos adjuntos, uno a la vez.

  Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.



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 seleccionar **Ajustes > 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 solicitar ayuda utilizando una de las siguientes opciones:

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

Gestione sus casos de soporte (vista previa)

Puede ver y gestionar los casos de soporte activos y resueltos directamente desde BlueXP. Es posible gestionar los casos asociados con su cuenta de NSS y con su empresa.

La gestión de casos está disponible como vista previa. Tenemos pensado perfeccionar esta experiencia y añadir mejoras en próximos lanzamientos. Envíenos sus comentarios mediante el chat en el producto.

Tenga en cuenta lo siguiente:

- La consola de gestión de casos en la parte superior de la página ofrece dos vistas:
  - La vista de la izquierda muestra el total de casos abiertos en los últimos 3 meses por la cuenta de usuario NSS que ha proporcionado.
  - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su compañía en función de su cuenta NSS de usuario.

  Los resultados de la tabla reflejan los casos relacionados con la vista seleccionada.

- Puede agregar o quitar columnas de interés y filtrar el contenido de columnas como prioridad y estado. Otras columnas proporcionan funciones de clasificación.

  Consulte los pasos a continuación para obtener más información.

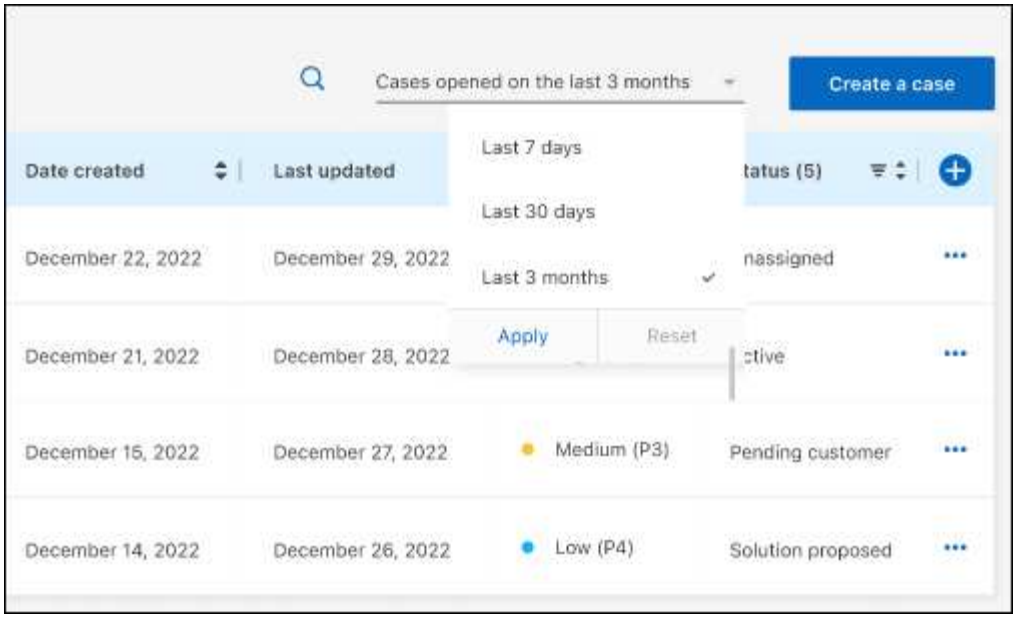
- En el nivel por caso, ofrecemos la posibilidad de actualizar las notas de un caso o cerrar un caso que no esté ya en estado cerrado o pendiente de cierre.

Pasos

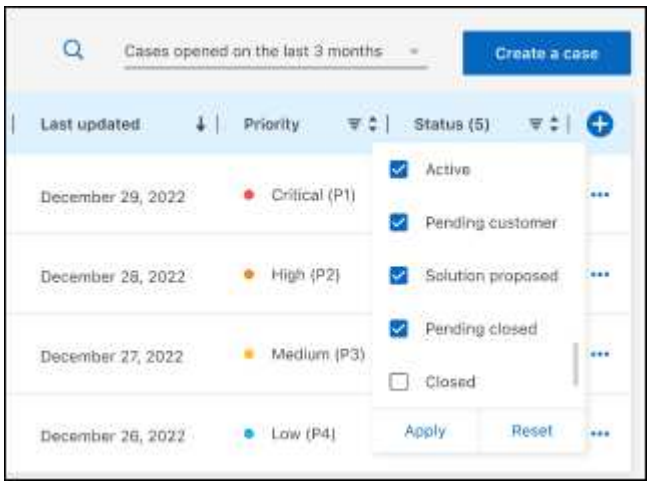
1. En BlueXP, selecciona **Ayuda > Soporte**.
2. Selecciona **Gestión de casos** y, si se te solicita, agrega tu cuenta de NSS a BlueXP.

   La página **Administración de casos** muestra casos abiertos relacionados con la cuenta NSS asociada con su cuenta de usuario de BlueXP. Esta es la misma cuenta NSS que aparece en la parte superior de la página **NSS Management**.

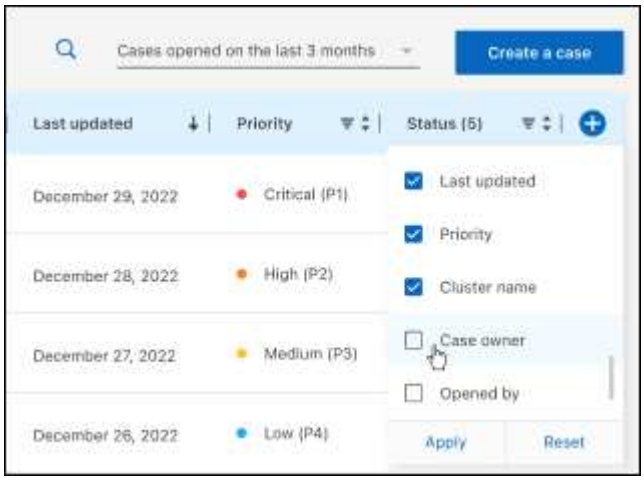
3. Si lo desea, puede modificar la información que se muestra en la tabla:
   - En **Casos de la organización**, selecciona **Ver** para ver todos los casos asociados a tu empresa.
   - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un marco de tiempo diferente.



- Filtre el contenido de las columnas.

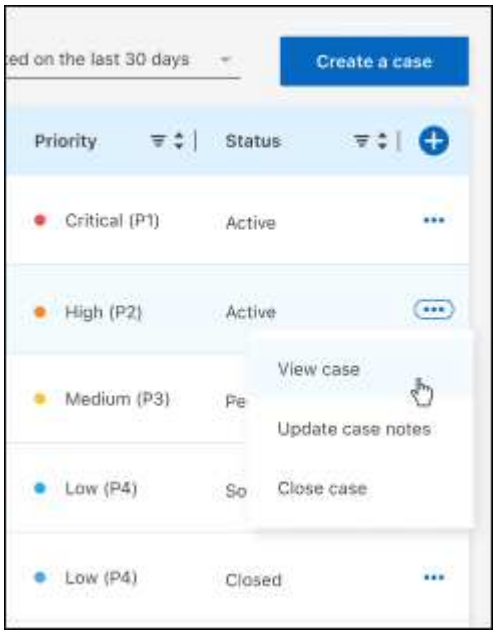


- Seleccione para cambiar las columnas que aparecen en la tabla y, a continuación, seleccione las columnas que desea mostrar.



4. Seleccione para gestionar un caso existente ••• y seleccione una de las opciones disponibles:
    - **Ver caso**: Ver todos los detalles sobre un caso específico.
    - **Actualizar notas de caso**: Proporcione detalles adicionales sobre su problema o seleccione **cargar archivos** para adjuntar hasta un máximo de cinco archivos.

      Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: Txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.
    - **Cerrar caso**: Proporciona detalles sobre por qué estás cerrando el caso y selecciona **Cerrar caso**.



Avisos legales

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

Derechos de autor

"https://www.netapp.com/company/legal/copyright/"

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.

"https://www.netapp.com/company/legal/trademarks/"

Estadounidenses

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

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

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"