Manos a la obra

BlueXP setup and administration

NetApp
August 29, 2025

Tabla de contenidos

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 de software como servicio (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

BlueXP proporciona un control unificado del almacenamiento en tu multinube híbrida y servicios de datos integrados para proteger, asegurar y optimizar los datos.

Control unificado del almacenamiento desde el lienzo de BlueXP

El lienzo *BlueXP* le permite descubrir, implementar y administrar el almacenamiento local y en la nube. El lienzo centraliza la gestión del almacenamiento.

Almacenamiento local y en cloud admitidos

BlueXP permite gestionar los siguientes tipos de almacenamiento desde el lienzo de BlueXP :

Soluciones de almacenamiento en cloud

- Amazon FSX para ONTAP de NetApp
- Azure NetApp Files
- Cloud Volumes ONTAP
- NetApp Volumes para Google Cloud

Almacenamiento de objetos y flash en las instalaciones

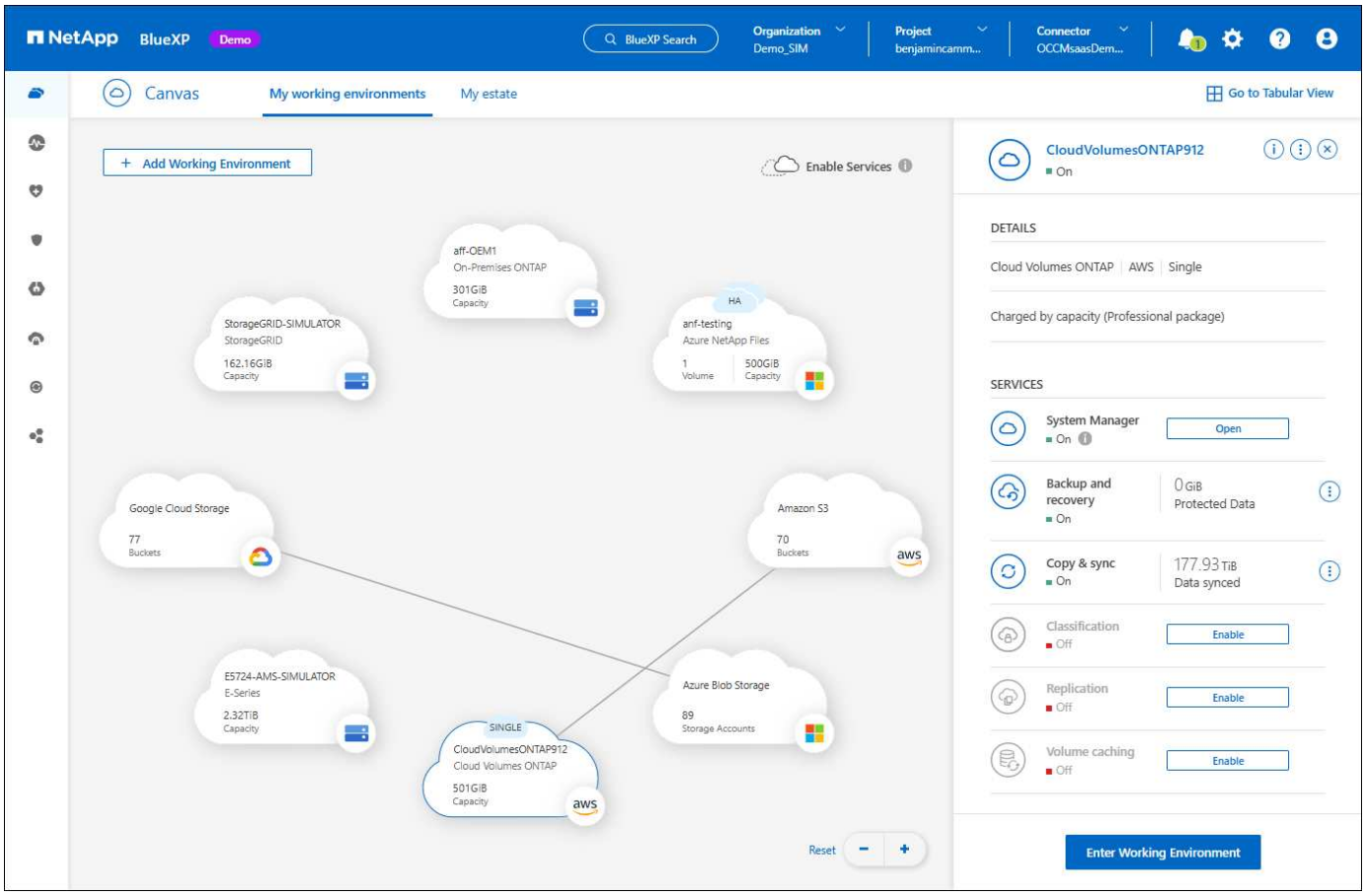
- Sistemas E-Series
- Clústeres ONTAP
- Sistemas StorageGRID

Almacenamiento de objetos en cloud

- Almacenamiento Amazon S3
- Almacenamiento de Azure Blob
- Google Cloud Storage

Gestión del almacenamiento desde entornos de trabajo

En el lienzo de BlueXP, los entornos de trabajo representan el almacenamiento detectado o implementado. Puede seleccionar un entorno de trabajo para integrarlo con los servicios de datos de BlueXP o administrar el almacenamiento, como agregar volúmenes.



Servicios integrados para proteger, asegurar y optimizar los datos

BlueXP incluye servicios de datos para proteger y mantener la disponibilidad de los datos en todo el almacenamiento.

Alertas BlueXP

Vea problemas relacionados con la capacidad, la disponibilidad, el rendimiento, la protección y la seguridad de su entorno de ONTAP.

Catálogo de automatización de BlueXP

Use soluciones generadas por scripts para automatizar la implementación e integración de productos y servicios de NetApp.

Backup y recuperación de BlueXP

Realice copias de seguridad y restaure datos locales y en la nube.

Clasificación de BlueXP

Consiga que los datos de aplicaciones y los entornos de cloud estén listos para la privacidad.

Copia y sincronización de BlueXP

Sincronice datos entre almacenes de datos locales y en la nube.

Asesor digital de BlueXP

Use análisis predictivos y soporte proactivo para optimizar su infraestructura de datos.

Cartera digital de BlueXP

Administre y supervise sus licencias y suscripciones.

Recuperación ante desastres de BlueXP

Protege las cargas de trabajo de VMware on-premises usando VMware Cloud on Amazon FSx para ONTAP como sitio de recuperación ante desastres.

Eficiencia económica de BlueXP

Identificar clusters con baja capacidad actual o prevista e implementar niveles de datos o recomendaciones adicionales de capacidad.

Protección contra ransomware de BlueXP

Detectar anomalías que puedan provocar ataques de ransomware. Proteja y recupere cargas de trabajo.

Replicación de BlueXP

Replicar datos entre sistemas de almacenamiento para dar soporte a backup y recuperación ante desastres

Actualizaciones de software de BlueXP

Automatice la evaluación, la planificación y la ejecución de las actualizaciones de ONTAP.

Consola de sostenibilidad de BlueXP

Analice la sostenibilidad de sus sistemas de almacenamiento.

Organización en niveles de BlueXP

Amplíe su almacenamiento ONTAP local a la nube.

Almacenamiento en caché de volúmenes de BlueXP

Cree un volumen de caché editable para acelerar el acceso a los datos o descargar el tráfico de volúmenes con un acceso frecuente.

Fábrica de cargas de trabajo BlueXP

Diseña, configura y opera cargas de trabajo clave con Amazon FSx for NetApp ONTAP.

"Obtenga más información sobre BlueXP y los servicios de datos disponibles"

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 utilices. "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 SaaS, un sistema de gestión de acceso y recursos, conectores que administran entornos de trabajo y habilitan los servicios en la nube de BlueXP , y diferentes modos de implementación para satisfacer los requisitos de su negocio.

Software como servicio

Se puede acceder a BlueXP a través de las API de la A "consola basada en web" y. Esta experiencia SaaS le permite acceder automáticamente a las últimas funciones a medida que se lanzan y cambiar fácilmente entre sus organizaciones, proyectos y conectores de BlueXP .

Gestión de identidades y accesos (IAM) de BlueXP

La gestión de acceso e identidad (IAM) de BlueXP es un modelo de gestión de recursos y accesos que proporciona gestión granular de recursos y permisos:

- Un nivel superior *ORGANIZATION* le permite administrar el acceso a través de sus diversos *PROYECTOS*
- *Folders* le permite agrupar proyectos relacionados
- La gestión de recursos permite asociar un recurso a una o más carpetas o proyectos
- La gestión de acceso permite asignar un rol a miembros de distintos niveles de la jerarquía de la organización

BlueXP IAM es compatible al usar BlueXP en modo estándar o restringido. Si usa BlueXP en modo privado, utilice una cuenta de BlueXP para administrar espacios de trabajo, usuarios y recursos.

- "Obtenga más información sobre BlueXP IAM"

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 le permite gestionar recursos y procesos en sus entornos locales y en la nube. Lo necesita para gestionar entornos de trabajo (por ejemplo, Cloud Volumes ONTAP) y para utilizar numerosos servicios de BlueXP .

"Más información sobre conectores".

Modos de implementación

BlueXP ofrece tres modos de despliegue. *Modo estándar* aprovecha el software BlueXP como capa de servicio (SaaS) para proporcionar una funcionalidad completa. Si su entorno tiene restricciones de seguridad y conectividad, *RESTRICTED MODE* y *PRIVATE MODE* limitan la conectividad saliente a la capa SaaS de BlueXP .

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

Certificación SOC 2 de tipo 2

Una firma de contadores públicos certificados independientes y un auditor de servicios examinaron a BlueXP y afirmaron que BlueXP logró informes SOC 2 Tipo 2 basados en los criterios de Servicios de Confianza aplicables.

"Consulte los informes de SOC 2 de NetApp"

Obtenga más información sobre los conectores BlueXP

Un *Connector* es el software de NetApp que se ejecuta en la red del cloud o en las instalaciones. Se utiliza para conectar los servicios de BlueXP a sus entornos de almacenamiento.

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:

- Amazon FSX para ONTAP de NetApp

  Algunas acciones requieren un conector o un enlace de fábrica de carga de trabajo BlueXP . "Aprenda qué acciones requieren un conector o enlace"

- 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 (solo licencias, la supervisión de suscripciones requiere un conector)

  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 sobre las opciones de descubrimiento y administración para clústeres ONTAP locales"

- Actualizaciones de software
- Sostenibilidad
- Fábrica de cargas de trabajo

Cuando se necesita un conector

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

- Alertas
- 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]
- Buckets de Google Cloud Storage
- Integración de clústeres de ONTAP en las instalaciones con servicios de datos de BlueXP
- 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 sus derechos bajo el EULA, podrían verse afectados negativamente.

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 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"

- 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

Comunicación con proveedores de cloud

El conector utiliza TLS 1,3 para todas las comunicaciones con AWS, Azure y Google Cloud.

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 instalar un conector

Puede instalar un conector directamente desde BlueXP, desde el marketplace de su proveedor de 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"
  - "Configurar permisos de nube para implementaciones locales"
- "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"

Es su responsabilidad actualizar las políticas de Connector a medida que se agregan nuevos permisos en las versiones posteriores. Si se requieren nuevos permisos, se mostrarán en las notas de la versión.

Actualizaciones de conectores

Normalmente actualizamos el software del conector cada mes para introducir nuevas funciones y para proporcionar mejoras de estabilidad. Mientras que la mayoría de los servicios y características de la plataforma BlueXP se ofrecen a través de software basado en SaaS, algunas características dependen de la versión del conector. Esto incluye la administración de Cloud Volumes ONTAP, la administración del clúster ONTAP local, la configuración y la 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 Connector cuando utilice el modo privado".

Mantenimiento del sistema operativo y los equipos virtuales

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

Tenga en cuenta que usted (cliente) no necesita detener ningún servicio en el host de Connector al aplicar actualizaciones de seguridad menores.

Si usted (cliente) necesita detener y luego iniciar la máquina virtual Connector, 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 y conectores

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.

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:

- Tienes un entorno multicloud (por ejemplo, AWS y Azure) y prefieres 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 organización de BlueXP para proporcionar servicios a sus clientes, mientras utiliza otra organización para prestar recuperación ante desastres a una de sus unidades de negocio. Cada organización tendría conectores separados.

Obtenga más información sobre los modos de implementación de BlueXP

BlueXP ofrece *modos de implementación* que le permiten satisfacer sus requisitos comerciales y de seguridad. El *modo estándar* aprovecha una capa de software como

servicio (SaaS) para proporcionar funcionalidad completa, mientras que el *modo restringido* y el *modo privado* están disponibles para organizaciones que tienen restricciones de conectividad.

Si bien BlueXP inhibe el flujo de tráfico, comunicación y datos cuando se usa el modo restringido o el modo privado, es su responsabilidad asegurarse de que su entorno (local y en la nube) cumpla con las regulaciones requeridas para su negocio.

Descripción general

Cada modo de implementación difiere en conectividad de salida, ubicación, instalación, autenticación, servicios de datos y métodos de cobro.

Modo estándar

Utiliza un servicio SaaS desde la consola web. Según los servicios de datos y las características que planee utilizar, un administrador de BlueXP crea uno o más conectores para administrar datos dentro de su entorno de nube híbrida.

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

Modo restringido

Instala un conector BlueXP en la nube (en una región gubernamental, soberana o comercial) y tiene conectividad de salida limitada a la capa SaaS de BlueXP.

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

Instala un conector BlueXP en sus instalaciones o en la nube (en una región segura, una región de nube soberana o una región comercial) y *no* tiene conectividad con la capa SaaS de BlueXP. Los usuarios acceden a la consola BlueXP proporcionada por el conector localmente, no a 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.

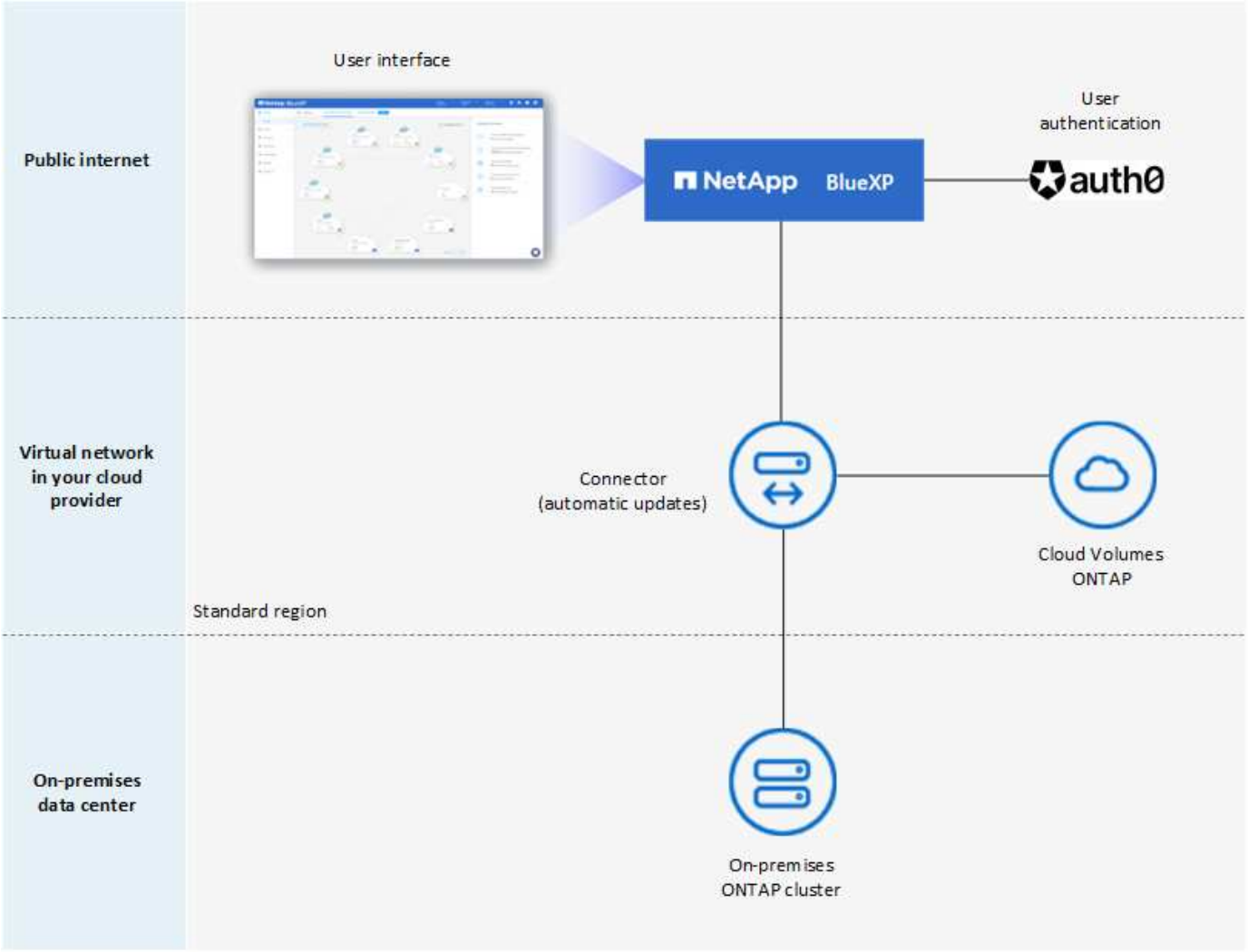
	Modo estándar	Modo restringido	Modo privado
¿Es necesaria una conexión a la capa SaaS de BlueXP?	Sí	Sólo saliente	No
¿Es necesaria una conexión con su proveedor de cloud?	Sí	Sí, dentro de la región	Sí, dentro de la región (si se utiliza Cloud Volumes ONTAP)
Instalación del conector	Desde BlueXP, Cloud Marketplace o instalación manual	Cloud Marketplace o instalación manual	Instalación manual

	Modo estándar	Modo restringido	Modo privado
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
Autenticación de múltiples factores	Disponible para usuarios locales	No disponible	No disponible
Almacenamiento y servicios de datos	Todos son compatibles	Muchos son compatibles	Se admiten varios
Opciones de licencia de servicios de datos	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

Puede instalar el conector mediante el asistente de configuración de BlueXP, AWS o Azure Marketplace, el SDK de Google Cloud o un instalador manual en un host Linux en su centro de datos o nube.

Actualizaciones de conectores

BlueXP proporciona actualizaciones automáticas del software Connector 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

BlueXP proporciona autenticación con inicios de sesión auth0 o 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.

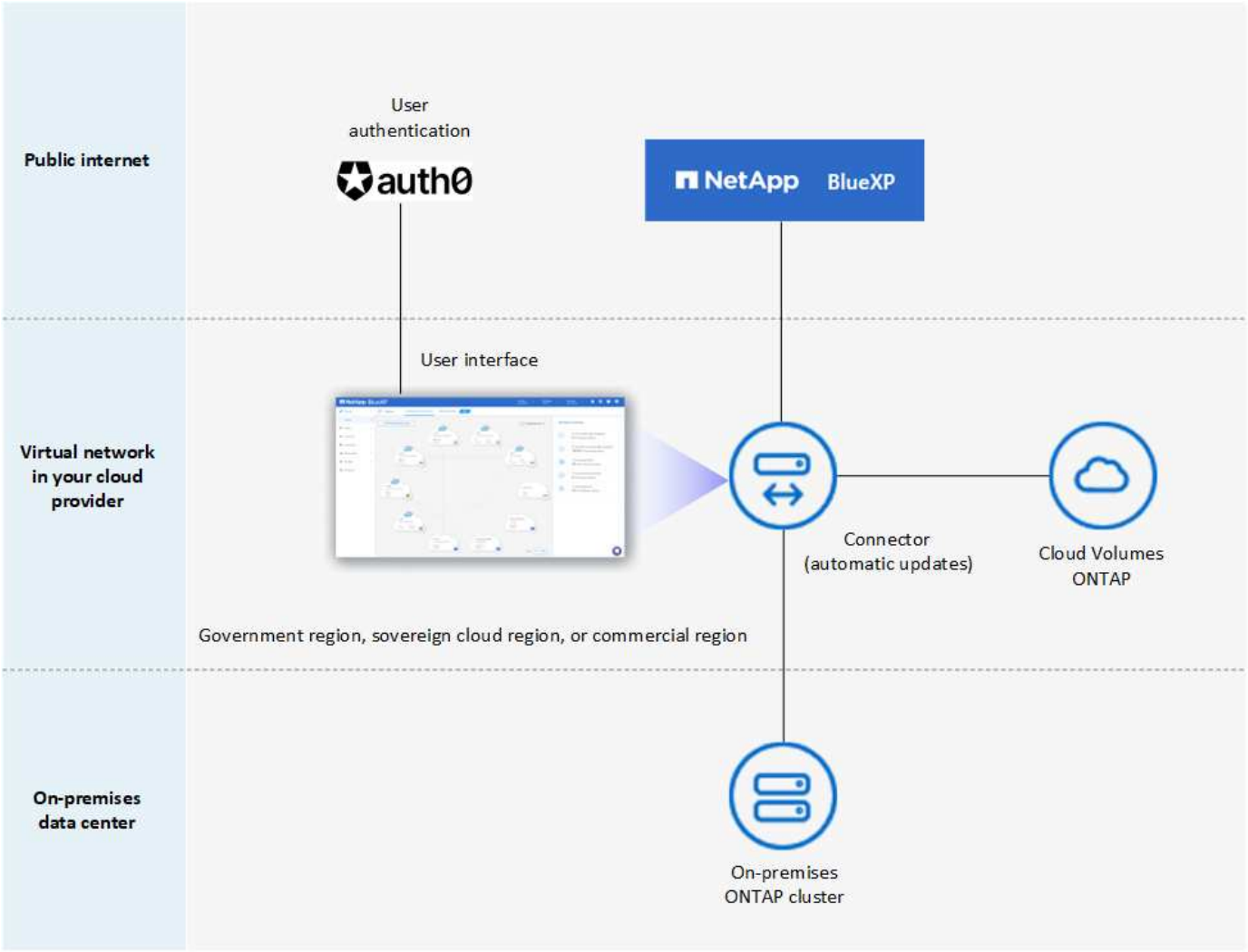
Cómo comenzar con el modo estándar

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

El conector requiere conectividad saliente a la capa SaaS de BlueXP para servicios de datos, actualizaciones de software, autenticación y transmisión de metadatos.

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

BlueXP proporciona actualizaciones automáticas del software Connector 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
Azure NetApp Files	Soporte completo
Backup y recuperación	Compatible con regiones gubernamentales y regiones comerciales con modo restringido. No compatible con regiones soberanas con modo restringido. En el modo restringido, la BlueXP backup and recovery solo admite la copia de seguridad y la restauración de datos de volumen ONTAP . "Consulte la lista de destinos de backup admitidos para los datos de ONTAP" En el modo restringido, la BlueXP backup and recovery solo admite la copia de seguridad y la restauración de datos de volumen ONTAP . "Consulte la lista de destinos de backup admitidos para los datos de ONTAP" No se admite la realización de copias de seguridad ni la restauración de datos de aplicaciones ni de máquinas virtuales.
Clasificación	Compatible en regiones gubernamentales con modo restringido. No se admite en regiones comerciales o en regiones soberanas con modo restringido.
Cloud Volumes ONTAP	Soporte completo
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 descubre un clúster local con un conector, la vista avanzada (Administrador del sistema) 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 organización, se le solicitará que cree su organización 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 nube.

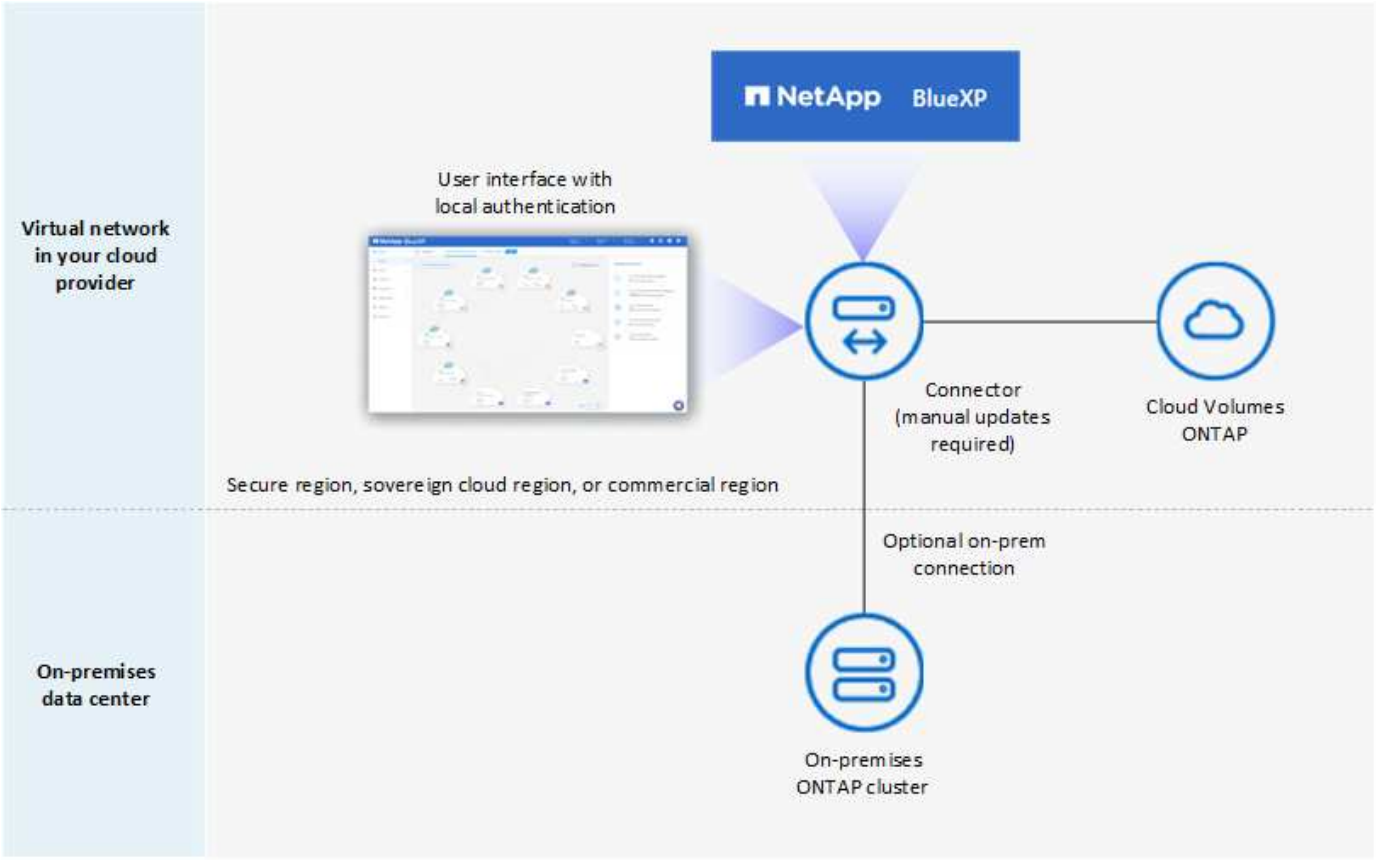
Tenga en cuenta que no puede cambiar la configuración del modo restringido después de que BlueXP cree la organización. No se puede activar el modo restringido más adelante y no se puede desactivar más adelante.

- "Aprenda a empezar a utilizar el modo restringido".

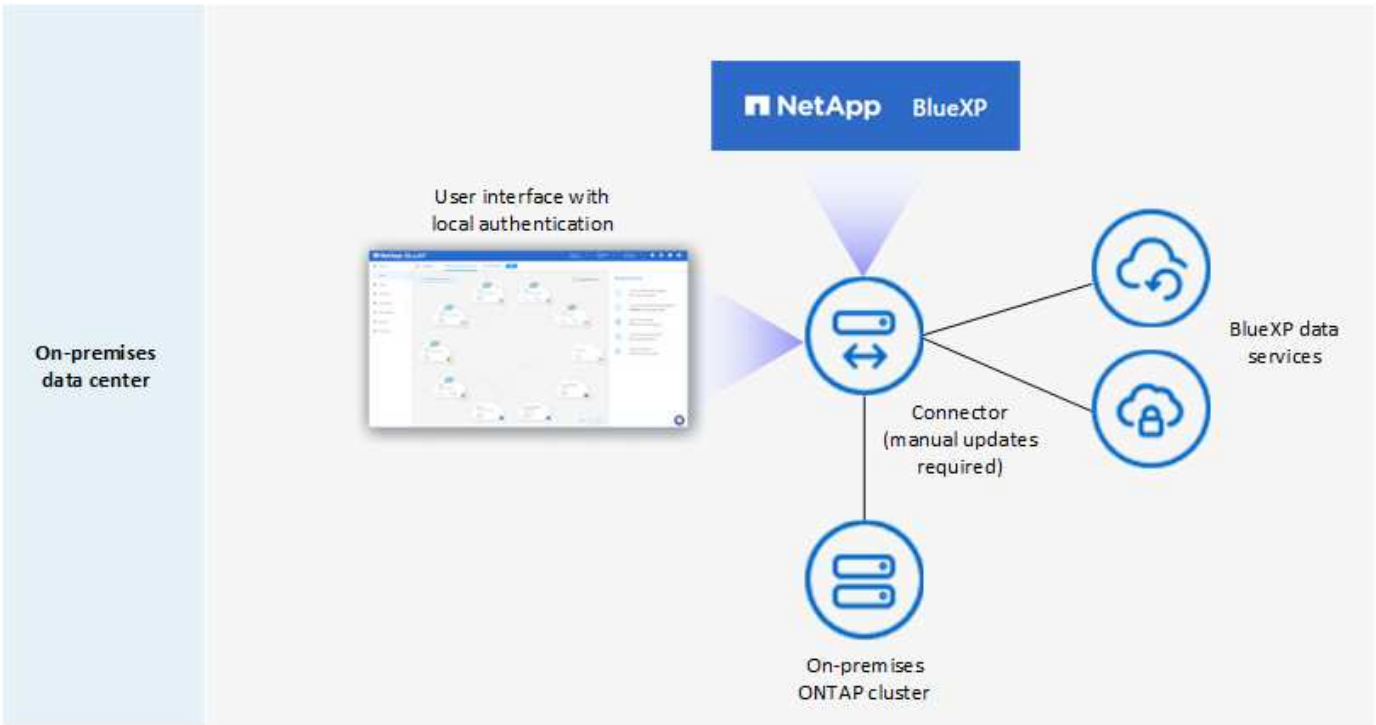
Modo privado

En el modo privado, puede instalar un conector en las instalaciones o en el cloud y, posteriormente, utilizar BlueXP para gestionar 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 donde el conector está instalado en las instalaciones, gestiona 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 el modo privado, el conector es compatible con el cloud o en las instalaciones.

Instalación del conector

Las instalaciones manuales de Connector son compatibles con su propio host Linux en el cloud o 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

Se puede acceder a la interfaz de usuario desde el conector que se implementa en la región de la nube o en las 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 las regiones comerciales de AWS y Azure. No compatible con Google Cloud ni con "Cloud secreto de AWS" , "Cloud secreto principal de AWS" , o "Azure IL6" En el modo privado, la BlueXP backup and recovery solo admite la copia de seguridad y la restauración de datos de volumen ONTAP . "Consulte la lista de destinos de backup admitidos para los datos de ONTAP" No se admite la realización de copias de seguridad ni la restauración de datos de aplicaciones ni de máquinas virtuales.
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.

Servicios compatibles	Notas
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 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, la BlueXP backup and recovery solo admite la copia de seguridad y la restauración de datos de volumen ONTAP . "Consulte la lista de destinos de backup admitidos para los datos de volúmenes ONTAP" No se admiten los backups y la restauración de los datos de aplicaciones y los datos de máquinas virtuales.
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. Debido a que no hay una conexión a Internet saliente disponible, debe cargar manualmente su archivo de licencia de Cloud Volumes ONTAP en la BlueXP digital wallet.

"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	No	No
	Amazon S3	No	No
	Azure Blob	No	No
	Azure NetApp Files	Sí	No
	Cloud Volumes ONTAP	Sí	Sí
	NetApp Volumes para Google Cloud	No	No
	Google Cloud Storage	No	No
	Clústeres de ONTAP locales	Sí	Sí
	E-Series	No	No
	StorageGRID	No	No

Área de producto	Servicio o característica BlueXP	Modo restringido	Modo privado
Servicios	Alertas	No	No
	Backup y recuperación	Síhttps://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["Consulte la lista de destinos de backup admitidos para los datos de volúmenes ONTAP"^]	Síhttps://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["Consulte la lista de destinos de backup admitidos para los datos de volúmenes ONTAP"^]
	Clasificación	Sí	Sí
	Copiar y sincronizar	No	No
	Asesor digital	No	No
	Cartera digital	Sí	Sí
	Recuperación tras siniestros	No	No
	Eficiencia económica	No	No
	Protección contra ransomware	No	No
	Replicación	Sí	Sí
	Actualizaciones de software	No	No
	Sostenibilidad	No	No
	Organización en niveles	No	No
	Almacenamiento en caché de volúmenes	No	No
	Fábrica de cargas de trabajo	No	No
* Características*	Gestión de identidades y accesos	Sí	Sí
	Credenciales	Sí	Sí
	Federación	Sí	No
	Autenticación de múltiples factores	Sí	No
	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)

Comience a utilizar BlueXP en modo estándar preparando la red para la consola de BlueXP, registrándose y creando una cuenta, creando opcionalmente un conector y suscribiéndose a NetApp Intelligent Services.

En el modo estándar, accede a una consola basada en web alojada como un producto de software como servicio (SaaS) de NetApp. Antes de comenzar, debe tener un entendimiento de "modos de despliegue" y. "Conectores"

"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.

"Regístrate y crea una organización"

Vaya a "Consola BlueXP" y regístrese. Se le dará la opción de crear una organización, pero puede omitir ese paso si lo invitan a una organización 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".

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.

Puede crear un conector en su red local o en la nube.

- "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 Datos Inteligentes de NetApp para gestionar el almacenamiento y los datos en Google Cloud, el Conector debe estar ejecutándose en Google Cloud .

"Suscríbase a los servicios inteligentes de NetApp (opcional)"

Suscríbase a los Servicios Inteligentes de NetApp desde la plataforma de su proveedor de nube para pagar por los servicios de datos con una tarifa por hora (PAYGO) o mediante un contrato anual. Los Servicios

Inteligentes de NetApp incluyen backup y recuperación, Cloud Volumes ONTAP, organización por niveles, protección contra ransomware y recuperación ante desastres. La clasificación está incluida en su suscripción sin coste adicional.

Prepare las redes para la consola de BlueXP

Al iniciar sesión y usar la consola web, BlueXP se conecta a varios endpoints para completar las acciones que usted inicia. Los equipos que acceden a la consola deben tener conexiones a estos endpoints.

Estos extremos se contactan en dos situaciones:

- Desde la computadora de un usuario al completar secciones de la "Consola BlueXP basada en Web" que está disponible como software como servicio (SaaS).
- Desde el equipo de un usuario al abrir un navegador web, introduzca la dirección IP del host del conector y, a continuación, inicie sesión y configure el conector. Estos pasos son necesarios si instala manualmente el conector.

Puntos finales	Específico
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	Este es el punto final que ingresa en su navegador web para utilizar la consola basada en web.
https://api.bluexp.netapp.com	La consola basada en web se comunica con este punto final para interactuar con la API para acciones relacionadas con autorización, licencias, suscripciones, credenciales, notificaciones y más.
https://aiq.netapp.com	Necesario para acceder al asesor digital.
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 punto final exacto depende de la región en la que implemente el conector. "Consulte la documentación de AWS para obtener más detalles." Sugerencia: "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.

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	Para el chat dentro del producto que le permite hablar con el soporte de NetApp.

Asegúrese de que el Conector tenga acceso a internet saliente para contactar con los puntos finales para las operaciones diarias. Siga los enlaces de la siguiente sección para encontrar la lista de estos puntos finales.

Información relacionada

- Prepare la conexión a redes para el conector
  - "Configure las redes de AWS"
  - "Configure las redes de Azure"
  - "Configure las redes de Google Cloud"
  - "Configurar la red local"
- Prepare las redes para los servicios de BlueXP

  Consulta la documentación para cada servicio de BlueXP.

  "Documentación de BlueXP"

Regístrate o inicia sesión en BlueXP

BlueXP es accesible desde una consola basada en Web. Cuando empieces a usar BlueXP, el primer paso es registrarte o iniciar sesión con tus credenciales del sitio de soporte de NetApp o credenciales de SSO en tu directorio corporativo.

Acerca de esta tarea

Cuando accedes a BlueXP por primera vez, BlueXP te permite registrarte o iniciar sesión con una de las siguientes opciones:

Inicio de sesión de BlueXP

Puedes registrarte creando un inicio de sesión de BlueXP. Este método de autenticación requiere que especifique su dirección de correo electrónico y una contraseña. Después de verificar su dirección de correo electrónico, puede iniciar sesión y, a continuación, crear una organización de BlueXP , si aún no pertenece a una.

Credenciales del sitio de soporte de NetApp (NSS)

Si tienes credenciales del sitio de soporte de NetApp existentes, no necesitas registrarte en BlueXP. Se inicia sesión con sus credenciales de NSS y, a continuación, BlueXP le solicita que cree una organización de BlueXP , si aún no pertenece a una.

Tenga en cuenta que la experiencia de contraseña predeterminada es un código de acceso único (OTP) a la dirección de correo electrónico registrada. Se genera un nuevo OTP con cada intento de inicio de sesión.

Conexión federada

Puede utilizar el inicio de sesión único para iniciar sesión con credenciales del directorio corporativo (identidad federada). El primer usuario de la cuenta de tu organización debe registrarse en BlueXP o iniciar sesión con las credenciales de NSS y, a continuación, configurar la federación de identidades. Después de eso, puede agregar miembros de su identidad corporativa a su organización. Esos usuarios pueden iniciar sesión con sus credenciales de SSO.

"Aprenda a usar la federación de identidades con BlueXP".

Pasos

1. Abra un explorador web y vaya al "Consola BlueXP"
2. Si tiene una cuenta en el sitio de soporte de NetApp o si ya ha configurado la federación de identidades, introduzca la dirección de correo electrónico asociada a su cuenta directamente en la página **Iniciar sesión**.

   En ambos casos, BlueXP le registrará como parte de este inicio de sesión inicial.

3. Si quieres registrarte creando un inicio de sesión de BlueXP, selecciona **Registrarse**.
   a. En la página **Registrarse**, ingrese la información requerida y seleccione **Siguiente**.

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

   b. Compruebe en su bandeja de entrada si hay un correo electrónico de NetApp que incluya instrucciones para verificar su dirección de correo electrónico.

      Es necesario realizar este paso para poder iniciar sesión en BlueXP.

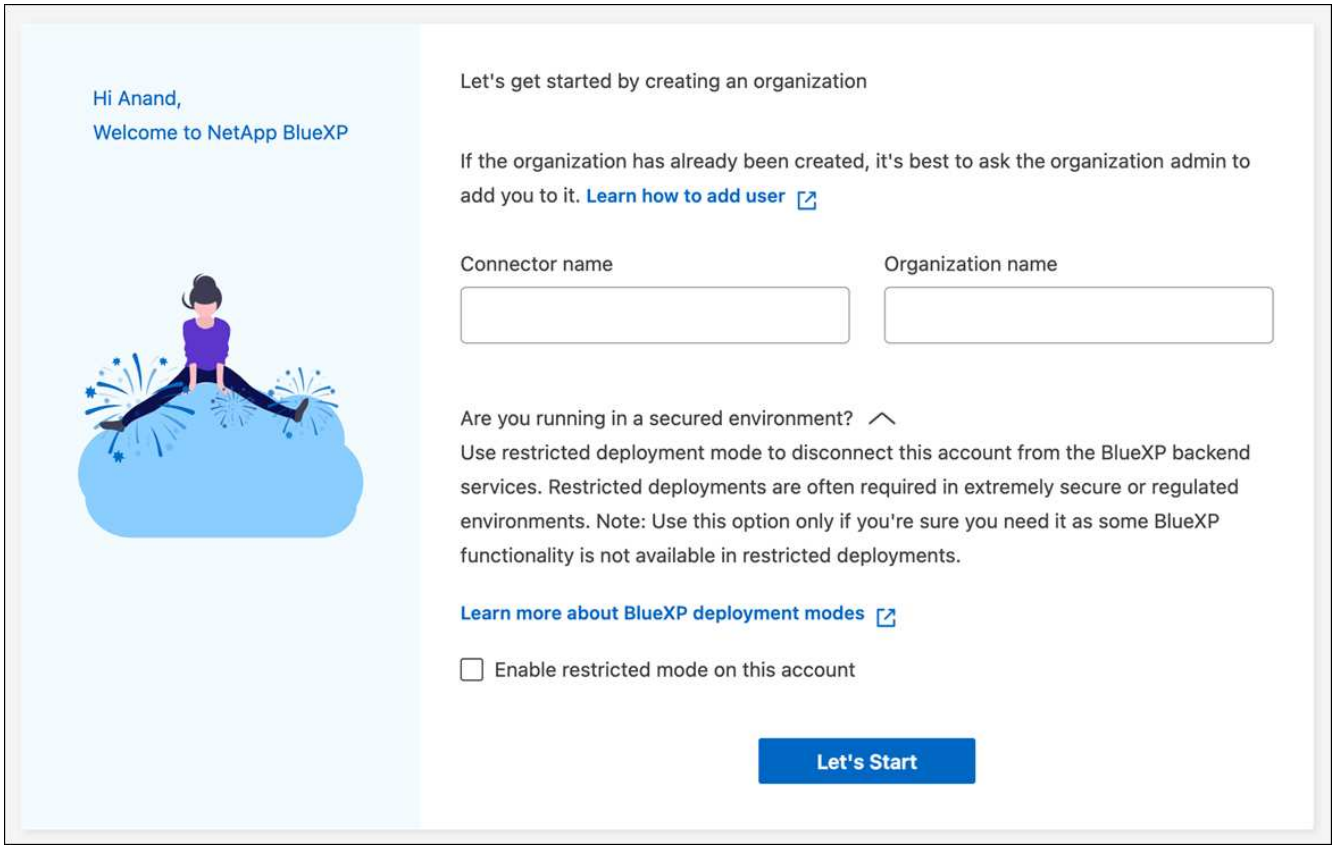
4. Después de iniciar sesión, revise el contrato de licencia para usuario final y acepte las condiciones.

   Si su cuenta de usuario no pertenece aún a una organización de BlueXP , se le pedirá que cree una.

5. En la página **Bienvenida**, ingrese un nombre para su organización de BlueXP .

   Una organización es el elemento de nivel superior en la gestión de acceso e identidad (IAM) de BlueXP . "Obtenga más información sobre BlueXP IAM".

   Si su empresa ya tiene una organización de BlueXP y desea unirse a ella, debe cerrar BlueXP y pedir al propietario que lo asocie con la organización. Una vez que el propietario le agregue, puede iniciar sesión y tendrá acceso a la cuenta. "Aprenda a agregar miembros a una organización existente".



6. Selecciona **Comenzar**.

Resultado

Ahora dispone de un inicio de sesión BlueXP y una organización. 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

Puede crear un conector en AWS directamente 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 tener un "Comprensión de los conectores".
- 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"

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.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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"

Pasos

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

   Esta directiva sólo contiene los permisos necesarios para iniciar la instancia de Connector en AWS desde

BlueXP. Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos a la instancia de Connector que permite al conector gestionar recursos de AWS. "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".
- Cuando BlueXP crea el conector, crea un rol de IAM y un perfil de instancia para la instancia. Este rol incluye permisos que permiten al conector administrar recursos de AWS. Debe asegurarse de que el rol se mantiene actualizado a medida que se agregan nuevos permisos en versiones posteriores. "Obtenga más información sobre la política de IAM para el conector".

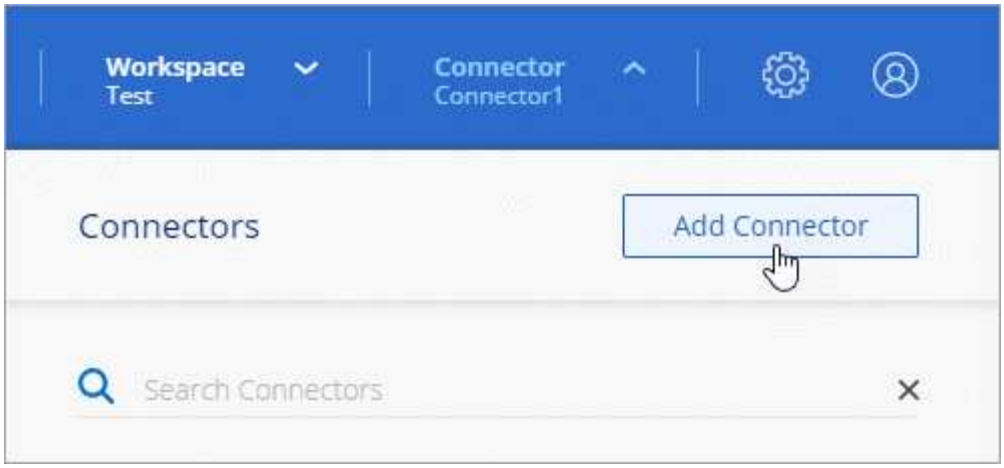
Antes de empezar

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

Puede crear un conector en AWS directamente 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 tener un "Comprensión de los conectores".
- 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.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Servidor proxy

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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

8 núcleos o 8 vCPU

RAM

32GB

Tipo de instancia de AWS EC2

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos t3.2xlarge.

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".

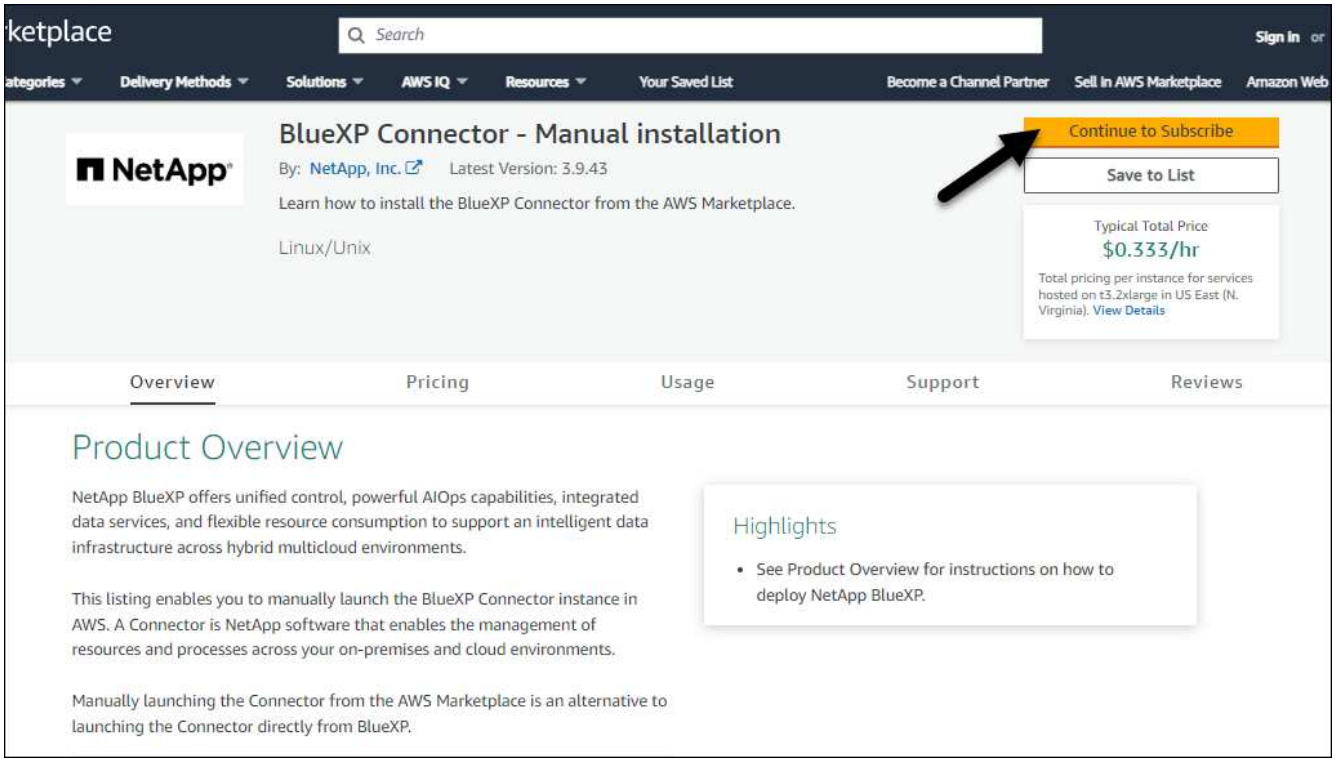
Antes de empezar

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

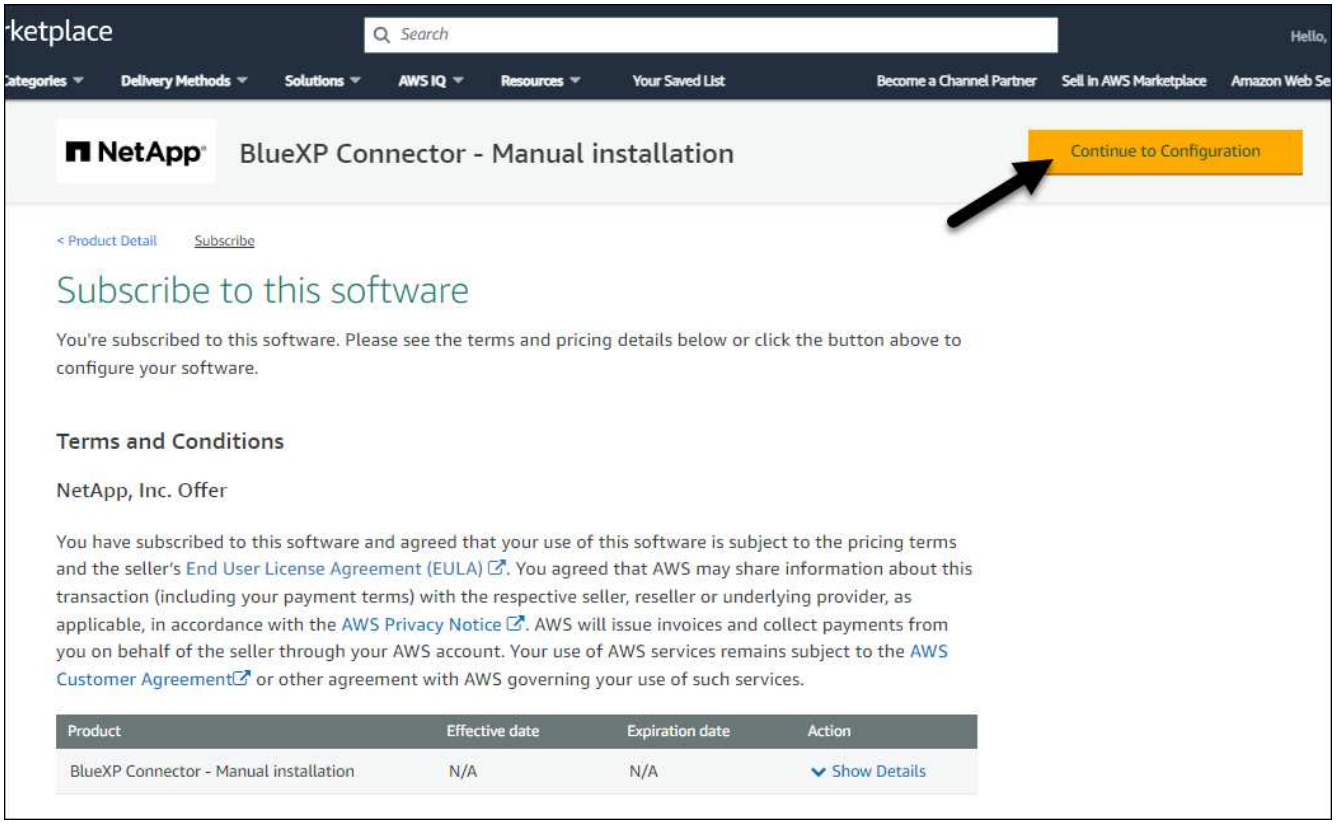
1. Vaya a la "Lista del conector BlueXP en el AWS Marketplace"
2. En la página de Marketplace, selecciona **Continuar para suscribirte**.



3. Para suscribirse al software, seleccione **Aceptar Términos**.

   El proceso de suscripción puede tardar unos minutos.

4. Una vez completado el proceso de suscripción, selecciona **Continuar con la configuración**.



5. En la página **Configurar este software**, asegúrate de haber seleccionado la región correcta y luego

selecciona **Continuar para iniciar**.

6. En la página **Iniciar este software**, 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**.

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

   - **Nombre y etiquetas**: Introduzca un nombre y etiquetas para la instancia.
   - **Aplicaciones e imágenes del sistema operativo**: Omita 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 (t3,2xlarge está preseleccionado y recomendado).
   - **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 grupo de seguridad que habilite los métodos de conexión necesarios para la instancia de conector: SSH, HTTP y HTTPS.

       "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.

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

   https://ipaddress

9. Después de iniciar sesión, configure el conector:
   a. Especifique la organización 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 organización 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

Puede instalar manualmente un conector en un host Linux ejecutándose 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 tener un "Comprensión de los conectores".
- 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.

> El Conector reserva el rango de UID y GID de 19000 a 19200. Este rango es fijo y no se puede modificar. Si algún software de terceros en su host utiliza UID o GID dentro de este rango, la instalación del Conector fallará. NetApp recomienda usar un host sin software de terceros para evitar conflictos.

Host dedicado

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

Host puede ser de cualquier arquitectura que cumpla con los siguientes requisitos de tamaño:

- CPU: 8 núcleos o 8 vCPU
- RAM: 32 GB

Hipervisor

Se requiere un hipervisor nativo o alojado que esté certificado para ejecutar un sistema operativo compatible.

Requisitos del sistema operativo y del contenedor

BlueXP admite el conector con los siguientes sistemas operativos cuando se utiliza BlueXP en modo estándar o en modo restringido. Antes de instalar el conector, se necesita una herramienta de orquestación de contenedores.

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Motor Docker 23.06 a 28.0.0.	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en 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.

Tipo de instancia de AWS EC2

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos t3.2xlarge.

Par de claves

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

Límite de salto de respuesta PUT al usar IMDSv2

Si IMDSv2 está habilitado en la instancia EC2 (este es el valor predeterminado para las nuevas instancias EC2), debe cambiar el límite de salto de respuesta PUT en la instancia a 3. Si no cambia el límite en la instancia de EC2, recibirá un error de inicialización de la interfaz de usuario cuando intente configurar el conector.

- "Requiere el uso de IMDSv2 en instancias de Amazon EC2"
- "Documentación de AWS: Cambie el límite de salto de respuesta PUT"

Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

BlueXP utiliza `/opt` para instalar el `/opt/application/netapp` directorio y su contenido.

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

BlueXP requiere este espacio en `/var` Porque Docker o Podman están diseñados para crear los contenedores dentro de este directorio. Específicamente, crearán contenedores en el `/var/lib/containers/storage` directorio. Los montajes externos o los enlaces simbólicos no

funcionan en este espacio.

Paso 2: Instale Podman o Docker Engine

Dependiendo del sistema operativo, se requiere Podman o Docker Engine antes de instalar el conector.

- Se requiere Podman para Red Hat Enterprise Linux 8 y 9.

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 1. Pasos

Podman

Siga estos pasos para instalar Podman y configurarlo para cumplir con los siguientes requisitos:

- Habilitar e iniciar el servicio podman.socket
- Instale python3
- Instalar el paquete podman-compose versión 1.0.6
- Agregue podman-compose a la variable de entorno PATH

> Al usar Podman, ajuste el puerto del servicio aardvark-dns (predeterminado: 53) después de instalar el Conector para evitar conflictos con el puerto DNS del host. Siga las instrucciones para configurar el puerto.

Pasos

1. Elimine el paquete podman-docker si está instalado en el host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale Podman.

   Podman está disponible en repositorios oficiales de Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

3. Active e inicie el servicio podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale el paquete de repositorio de EPEL si aún no está disponible en su sistema.

   Este paso es necesario porque podman-compose está disponible en el repositorio Extra Packages for Enterprise Linux (EPEL).

   Para Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Instale el paquete podman-compose 1,0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   Con el `dnf install` El comando cumple con los requisitos para agregar podman-compose a la variable de entorno PATH. El comando installation agrega podman-compose a /usr/bin, que ya está incluido en el `secure_path` opción en el host.

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

   Asegúrese de seguir los pasos para instalar una versión específica de Docker Engine. Al instalar la versión más reciente se instalará una versión de Docker no compatible con BlueXP.

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 3: 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 desde los equipos cuando se utiliza la consola basada en web de BlueXP

Los equipos que acceden a la consola de BlueXP desde un navegador web deben tener la capacidad de contactar con varios puntos finales. Necesitará utilizar la consola BlueXP para configurar el conector y para utilizar el día a día de BlueXP .

"Prepare las redes para la consola de BlueXP ".

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://mysupport.netapp.com
- https://signin.b2c.NetApp.com (este punto final es la URL de CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- Para obtener imágenes, el instalador necesita acceder a uno de estos dos conjuntos de puntos finales:
  - Opción 1 (recomendado):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Opción 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

    Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

  - Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
  - El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
  - Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar

los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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://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.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Servidor proxy

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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 4: 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 5: 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.

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

> No se puede configurar un certificado para un servidor proxy transparente al instalar el Conector manualmente. Si necesita configurar un certificado para un servidor proxy transparente, debe usar la Consola de mantenimiento después de la instalación. Obtenga más información sobre el "Consola de mantenimiento del conector".

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. 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.

2. 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.

3. Asigne permisos para ejecutar el script.

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

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

4. 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>
```

Necesitará agregar la información del proxy si su red requiere uno para acceder a internet. Puede agregar un proxy transparente o explícito. Los parámetros --proxy y --cacert son opcionales y no se le solicitará que los agregue. Si tiene un servidor proxy, deberá introducir los parámetros como se muestra.

A continuación se muestra un ejemplo de configuración de un servidor proxy explícito con un certificado firmado por una CA:

```
 ./BlueXP-Connector-Cloud-v3.9.40--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 un \ como se muestra anteriormente.
  - BlueXP no admite nombres de usuario ni contraseñas que incluyan el carácter @.
  - Si la contraseña incluye alguno de los siguientes caracteres especiales, debe escapar de ese carácter especial preponiéndolo con una barra diagonal inversa: & O !

    Por ejemplo:

    http://bxpproxyuser:netapp1\!@address:3128

    --cacert especifica un certificado firmado por CA que se utilizará para el acceso HTTPS entre el conector y el servidor proxy. Este parámetro es necesario para servidores proxy HTTPS, servidores proxy de interceptación y servidores proxy transparentes.

  A continuación se muestra un ejemplo de configuración de un servidor proxy transparente. Al configurar un proxy transparente, no es necesario definir el servidor proxy. Solo se agrega un certificado firmado por una CA al host del conector:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. Si usó Podman, necesitará ajustar el puerto aardvark-dns.
   a. SSH a la máquina virtual del conector BlueXP.
   b. Abra el archivo podman */usr/share/containers/containers.conf* y modifique el puerto seleccionado para el servicio DNS de Aardvark. Por ejemplo, cámbielo a 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. Reinicie la máquina virtual del conector.
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 organización 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**.

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 6: 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

Puede instalar un conector en Azure directamente desde BlueXP . Para crear un conector en Azure desde BlueXP , debe configurar la red, preparar un rol de Azure para usarlo para implementar el conector y, a continuación, implementar el conector.

Antes de empezar

- Usted debe tener un "Comprensión de los conectores".
- 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.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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 una política de implementación de Connector (rol personalizado)

Debe crear un rol personalizado que tenga permisos para desplegar Connector en Azure.

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.

Una vez que BlueXP implementa la máquina virtual Connector en Azure, habilita una "identidad administrada asignada por el sistema" en la máquina virtual, crea automáticamente la función que necesita y la asigna a la máquina virtual. El rol creado automáticamente proporciona a BlueXP los permisos necesarios para gestionar recursos y procesos dentro de esa suscripción de Azure. "Revise cómo BlueXP utiliza los permisos".

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 a la máquina virtual de Connector que permite al conector gestionar los recursos de Azure.

```
{
    "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

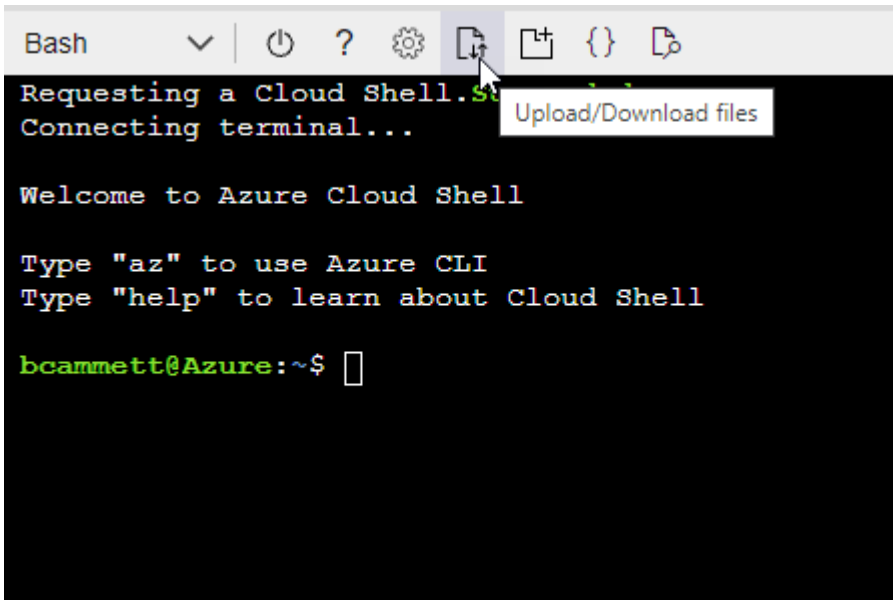
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],
```

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.

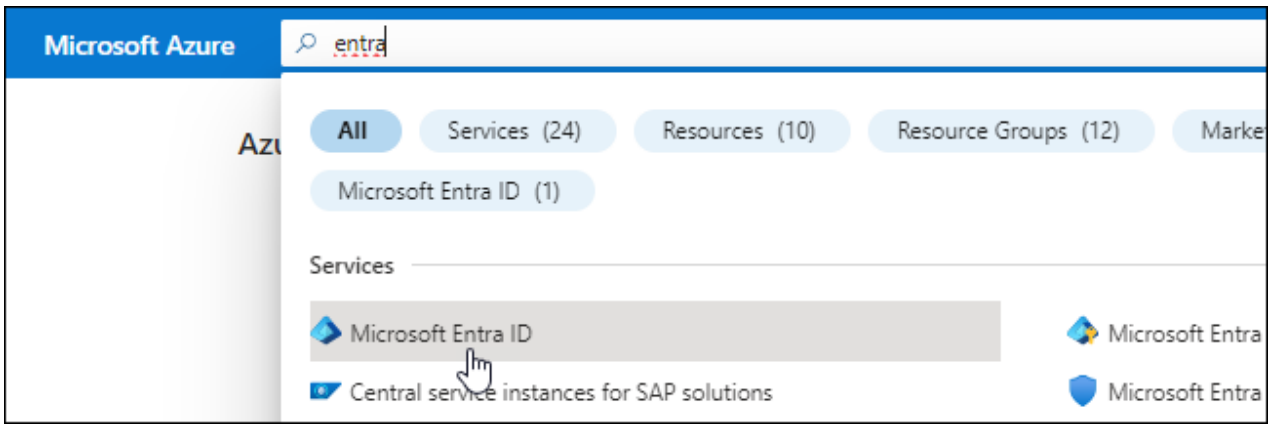
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

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**.

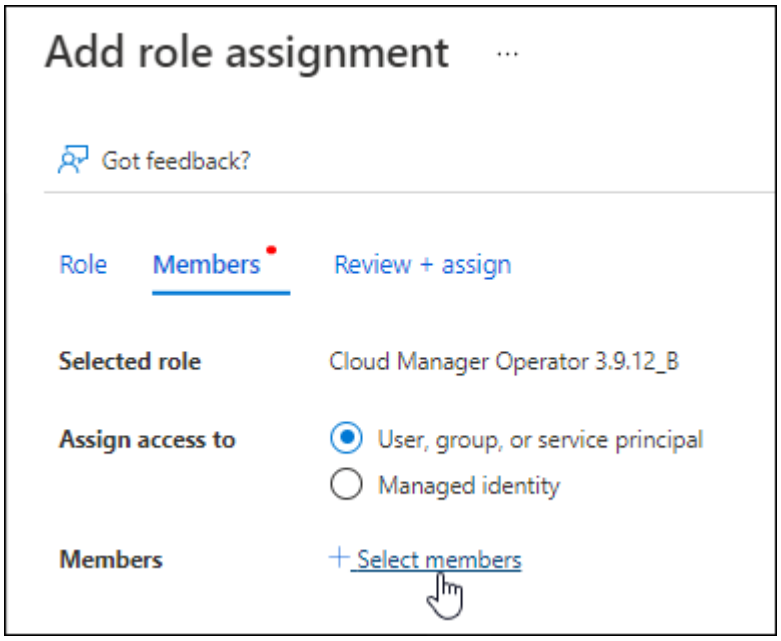
   Ha creado la aplicación AD y el director de servicio.

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:

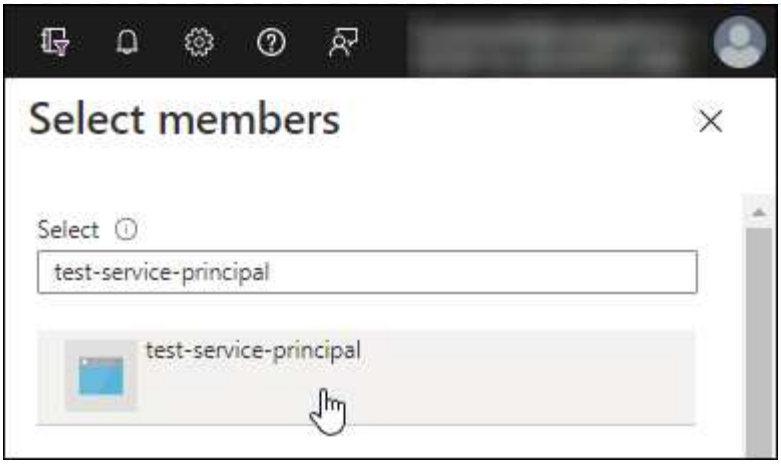
   a. Mantener seleccionado **Usuario, grupo o principal de servicio**.

   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**.

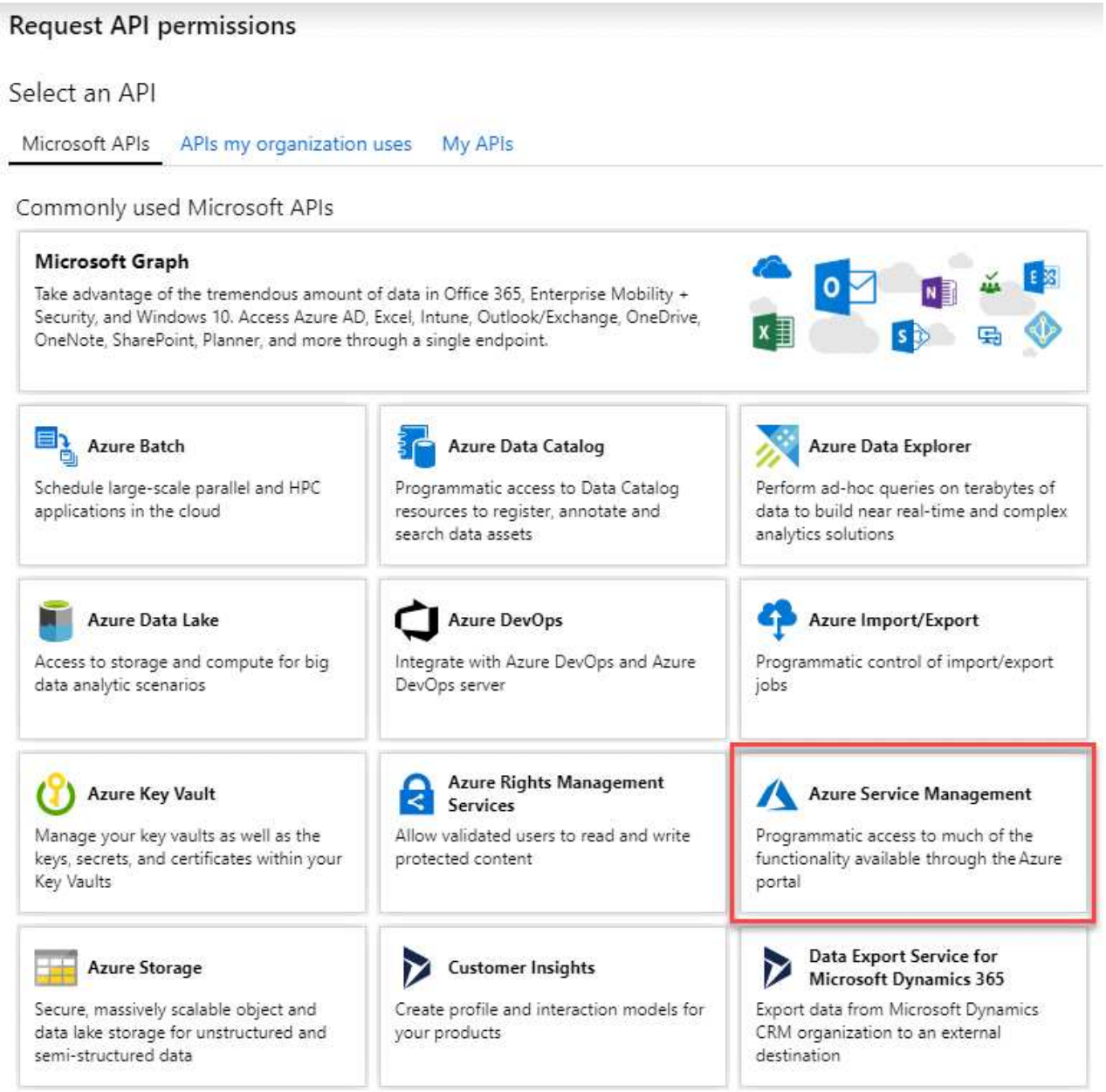
6. Haga clic en **revisar + asignar**.

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

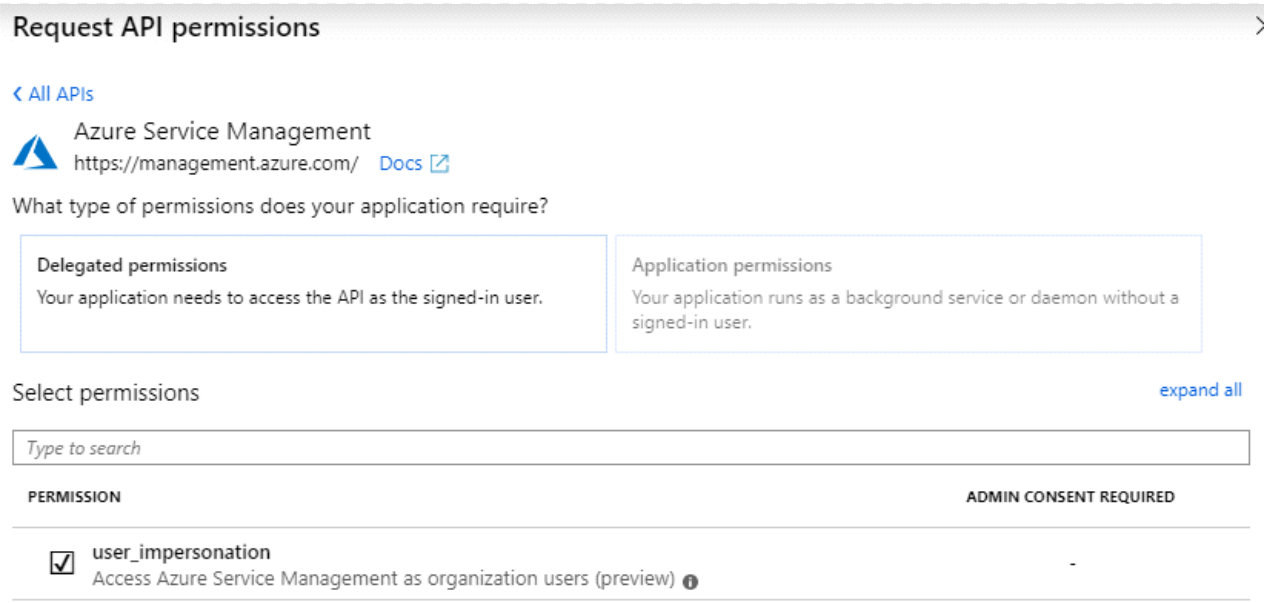
   Si desea administrar recursos en varias suscripciones de Azure, debe vincular el principal de servicio a cada una de esas suscripciones. Por ejemplo, BlueXP te permite seleccionar la suscripción que desees utilizar al implementar Cloud Volumes ONTAP.

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**.

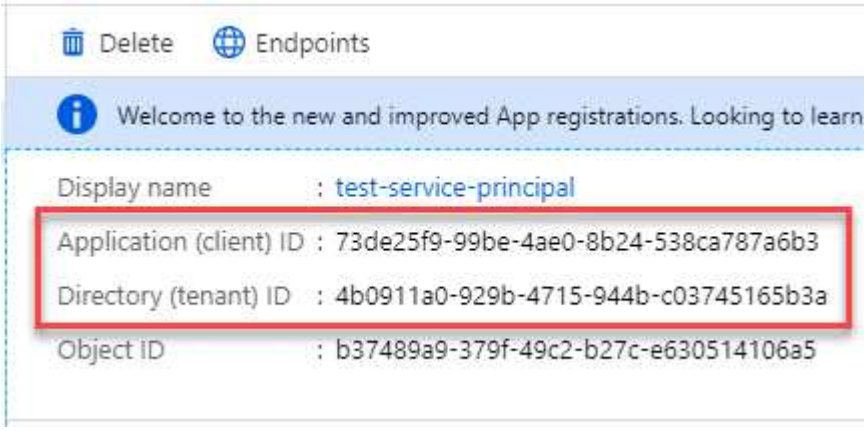


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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".
- Cuando BlueXP pone en marcha Connector, crea un rol personalizado y lo asigna a la máquina virtual Connector. Este rol incluye permisos que permiten al conector administrar recursos de Azure. Debe asegurarse de que el rol se mantiene actualizado a medida que se agregan nuevos permisos en versiones posteriores. "Obtenga más información sobre el rol personalizado del 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.

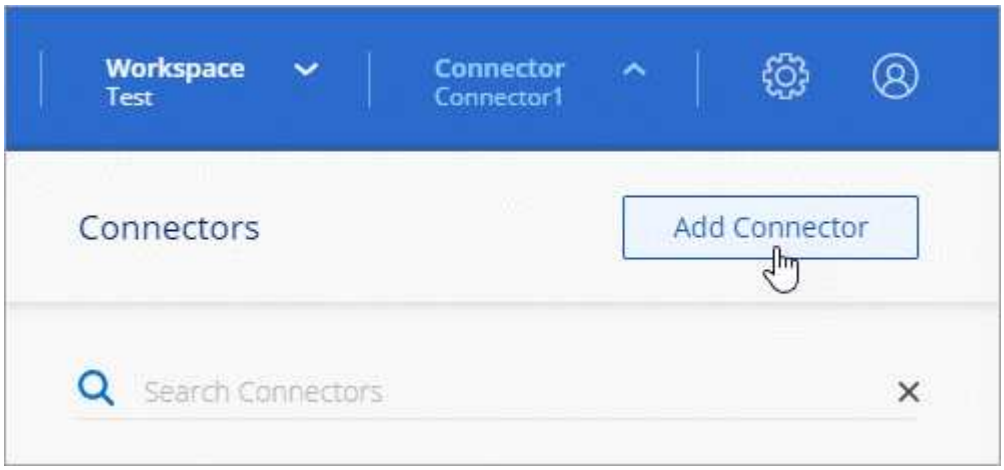
  "Obtenga más información sobre cómo conectarse a una máquina virtual de Linux en Azure"

- 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

Puede crear un conector en Azure directamente 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 tener un "Comprensión de los conectores".
- Revisar "Limitaciones del conector" .

Paso 1: Configurar redes

Asegúrese de que la ubicación de red donde planea instalar el Conector admita los siguientes requisitos. Estos requisitos permiten que el Conector administre recursos en su 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.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Servidor proxy

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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"

Implemente los requisitos de red después de crear el conector.

Paso 2: Revise los requisitos de VM

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

CPU

8 núcleos o 8 vCPU

RAM

32GB

Tamaño de la máquina virtual de Azure

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos Standard_D8s_v3.

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

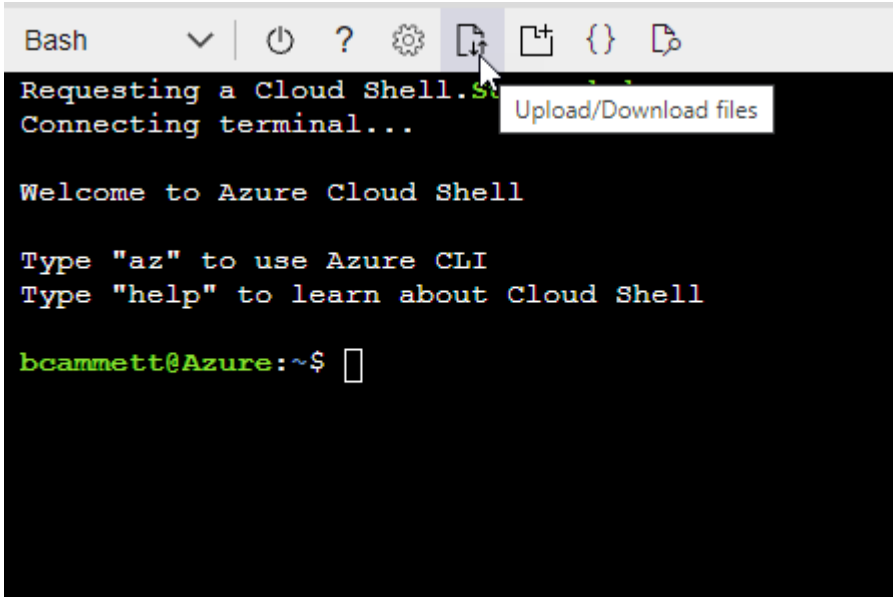
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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

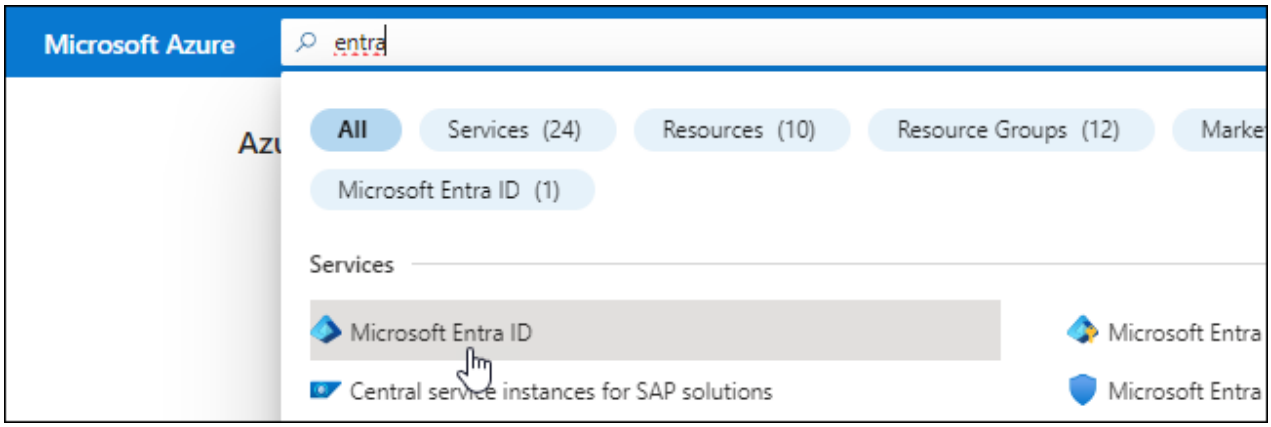
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

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.

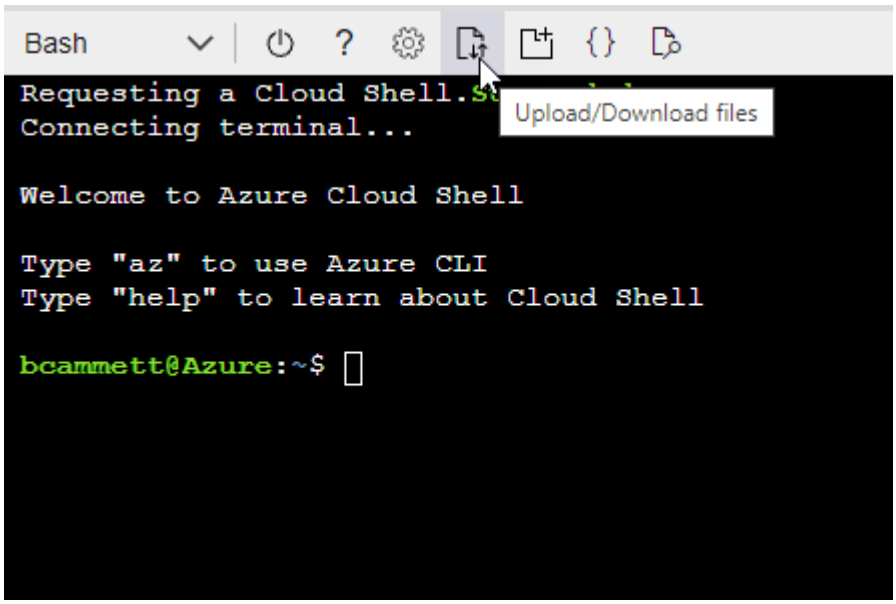
   ejemplo

```
"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:

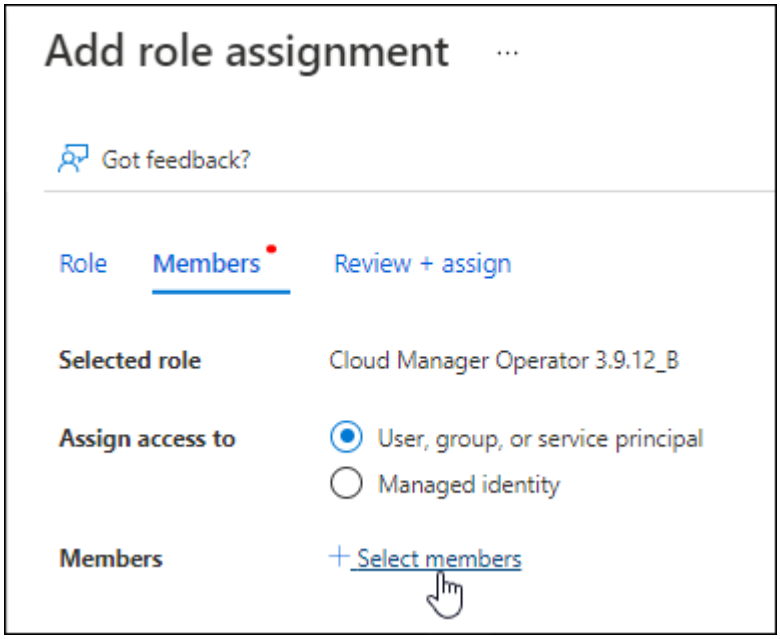
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

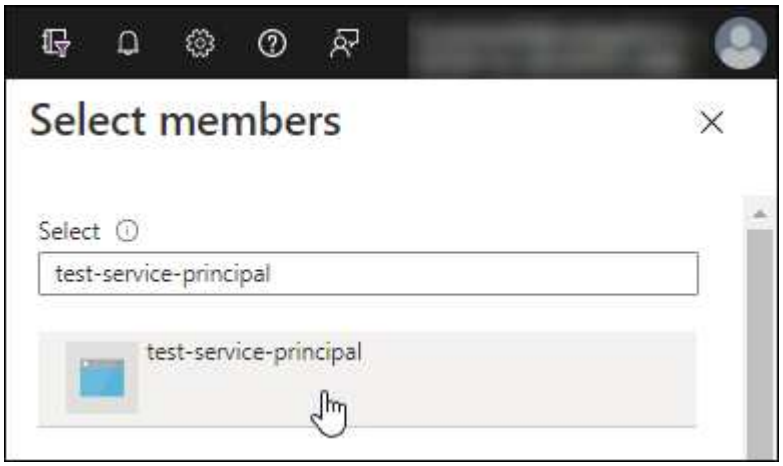
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**,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

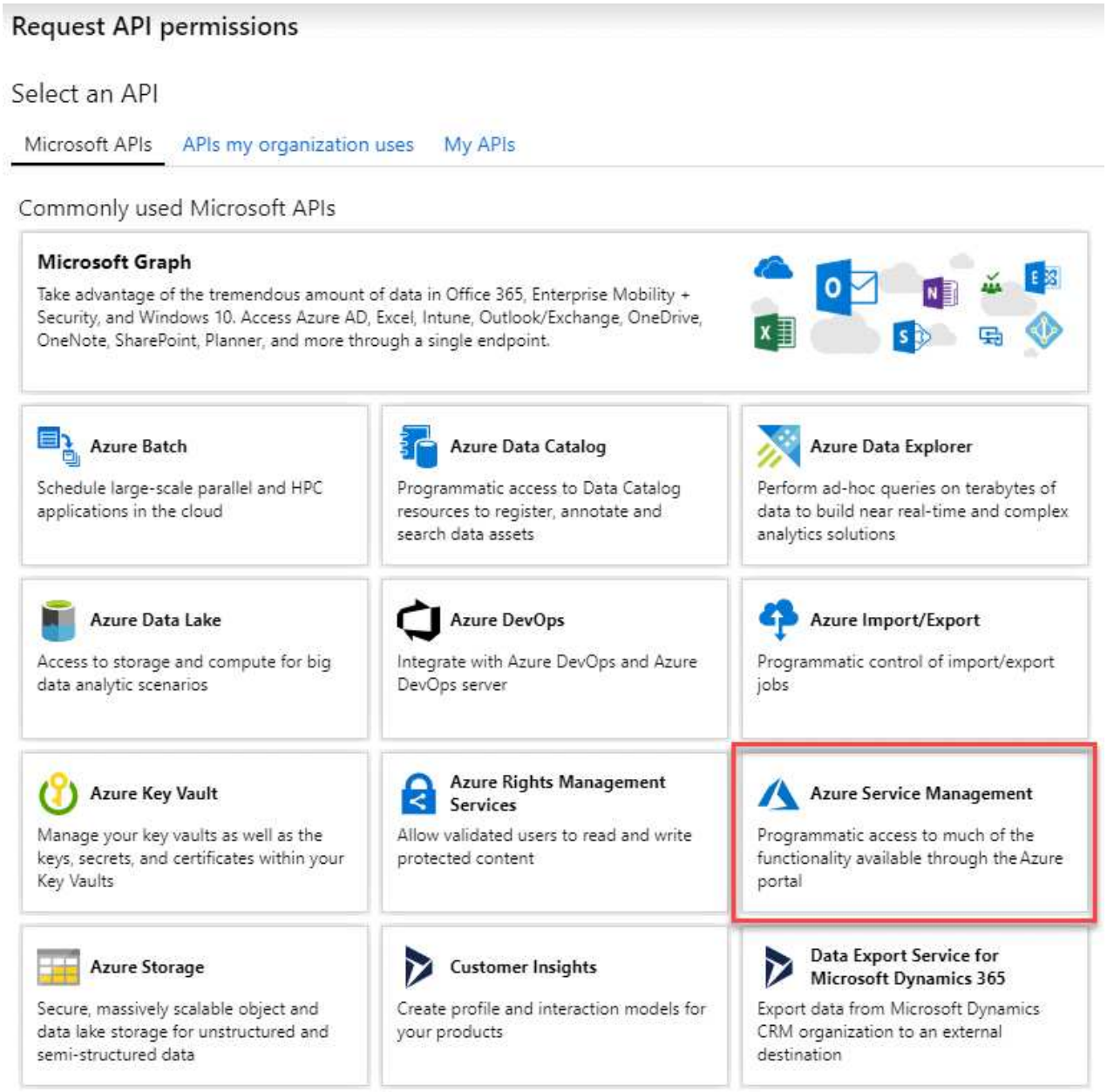
f. Seleccione **revisar + asignar**.

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

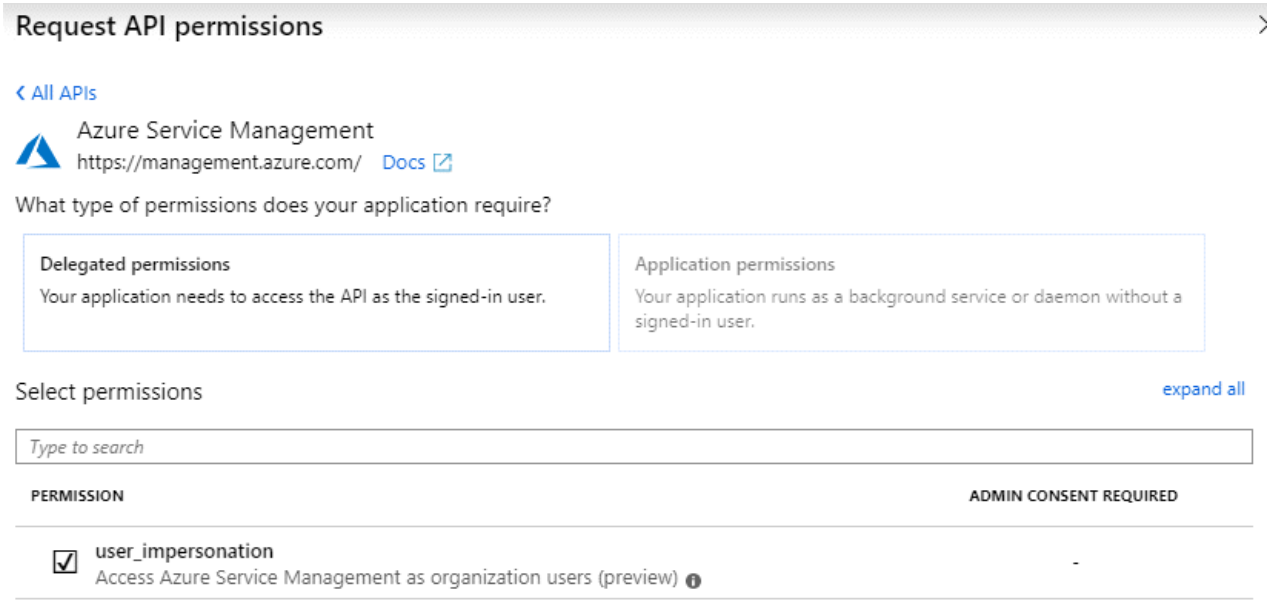
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. BlueXP le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

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**.

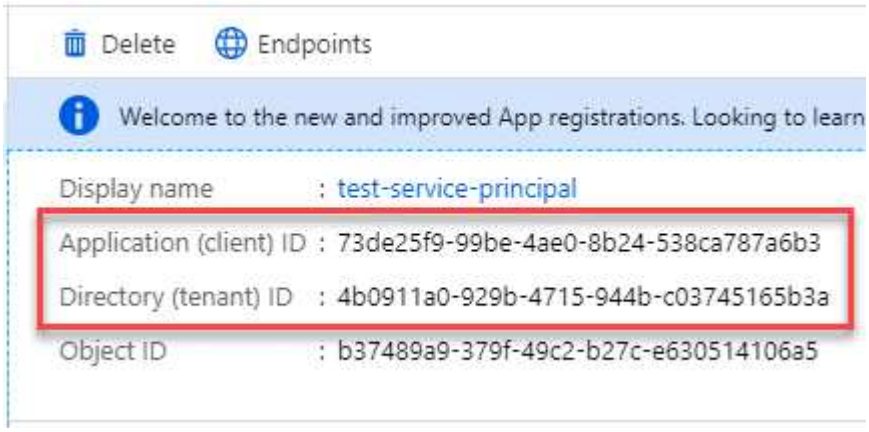


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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

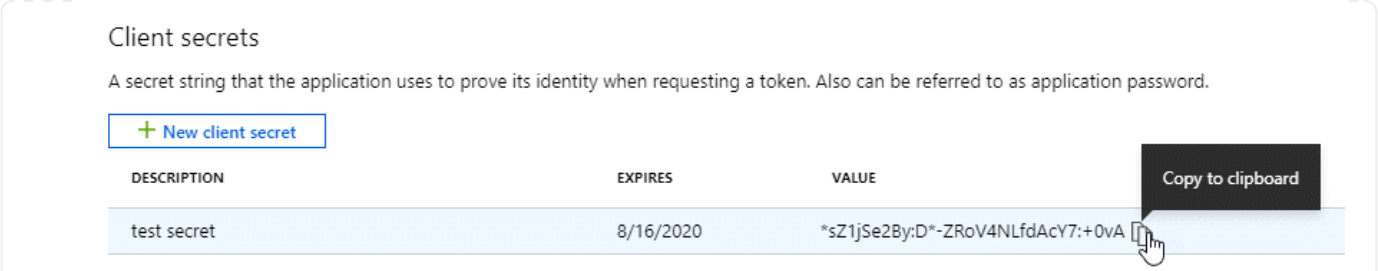
1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Paso 4: Crear el conector

Inicie Connector directamente desde Azure Marketplace.

Acerca de esta tarea

Al crear el conector desde Azure Marketplace, se configura una máquina virtual 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 Standard_D8s_v3.
- **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. Debería ver la máquina virtual y el software del conector ejecutándose 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 organización 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.

      Mantenga el modo restringido deshabilitado para usar 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. En ese caso, "Siga los pasos para comenzar con BlueXP en modo restringido" .

   d. Selecciona **Comenzar**.

Resultado

Ahora ha instalado el Conector y lo ha configurado con su organización 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.

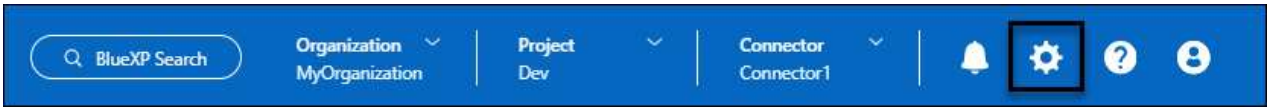
El futuro

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

Un conector es el software NetApp que se ejecuta en su red de cloud o en las instalaciones que le da la posibilidad de usar todas las funciones y servicios de BlueXP . Una de las opciones de instalación disponibles es instalar manualmente el software Connector en un host Linux que se ejecuta 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 tener un "Comprensión de los conectores".
- 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.

> El Conector reserva el rango de UID y GID de 19000 a 19200. Este rango es fijo y no se puede modificar. Si algún software de terceros en su host utiliza UID o GID dentro de este rango, la instalación del Conector fallará. NetApp recomienda usar un host sin software de terceros para evitar conflictos.

Host dedicado

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

Host puede ser de cualquier arquitectura que cumpla con los siguientes requisitos de tamaño:

- CPU: 8 núcleos o 8 vCPU
- RAM: 32 GB

Hipervisor

Se requiere un hipervisor nativo o alojado que esté certificado para ejecutar un sistema operativo compatible.

Requisitos del sistema operativo y del contenedor

BlueXP admite el conector con los siguientes sistemas operativos cuando se utiliza BlueXP en modo estándar o en modo restringido. Antes de instalar el conector, se necesita una herramienta de orquestación de contenedores.

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Motor Docker 23.06 a 28.0.0.	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en 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.

Tamaño de la máquina virtual de Azure

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos Standard_D8s_v3.

Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

BlueXP utiliza `/opt` para instalar el `/opt/application/netapp` directorio y su contenido.

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

BlueXP requiere este espacio en `/var` Porque Docker o Podman están diseñados para crear los contenedores dentro de este directorio. Específicamente, crearán contenedores en el `/var/lib/containers/storage` directorio. Los montajes externos o los enlaces simbólicos no funcionan en este espacio.

Paso 2: Instale Podman o Docker Engine

Dependiendo del sistema operativo, se requiere Podman o Docker Engine antes de instalar el conector.

- Se requiere Podman para Red Hat Enterprise Linux 8 y 9.

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 2. Pasos

Podman

Siga estos pasos para instalar Podman y configurarlo para cumplir con los siguientes requisitos:

- Habilitar e iniciar el servicio podman.socket
- Instale python3
- Instalar el paquete podman-compose versión 1.0.6
- Agregue podman-compose a la variable de entorno PATH

> Al usar Podman, ajuste el puerto del servicio aardvark-dns (predeterminado: 53) después de instalar el Conector para evitar conflictos con el puerto DNS del host. Siga las instrucciones para configurar el puerto.

Pasos

1. Elimine el paquete podman-docker si está instalado en el host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale Podman.

   Podman está disponible en repositorios oficiales de Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

3. Active e inicie el servicio podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale el paquete de repositorio de EPEL si aún no está disponible en su sistema.

   Este paso es necesario porque podman-compose está disponible en el repositorio Extra Packages for Enterprise Linux (EPEL).

   Para Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Instale el paquete podman-compose 1,0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   Con el `dnf install` El comando cumple con los requisitos para agregar podman-compose a la variable de entorno PATH. El comando installation agrega podman-compose a /usr/bin, que ya está incluido en el `secure_path` opción en el host.

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

   Asegúrese de seguir los pasos para instalar una versión específica de Docker Engine. Al instalar la versión más reciente se instalará una versión de Docker no compatible con BlueXP.

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 3: 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 desde los equipos cuando se utiliza la consola basada en web de BlueXP

Los equipos que acceden a la consola de BlueXP desde un navegador web deben tener la capacidad de contactar con varios puntos finales. Necesitará utilizar la consola BlueXP para configurar el conector y para utilizar el día a día de BlueXP .

"Prepare las redes para la consola de BlueXP ".

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://mysupport.netapp.com
- https://signin.b2c.NetApp.com (este punto final es la URL de CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- Para obtener imágenes, el instalador necesita acceder a uno de estos dos conjuntos de puntos finales:
  - Opción 1 (recomendado):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Opción 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

    Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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.

Puntos finales	Específico
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Servidor proxy

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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 4: Configure los permisos de implementación de Connector

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.

Cree un rol personalizado para el despliegue de Connector

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

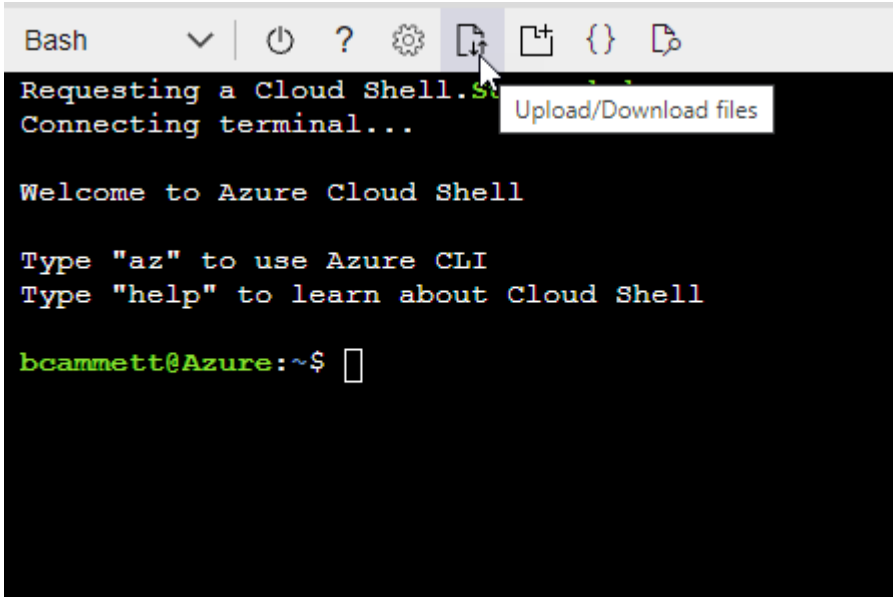
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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

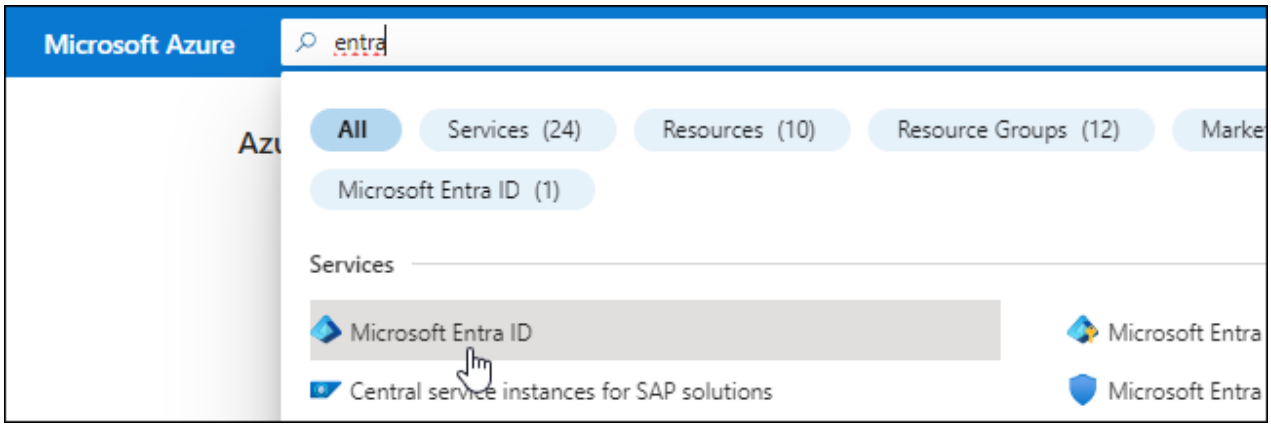
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

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.

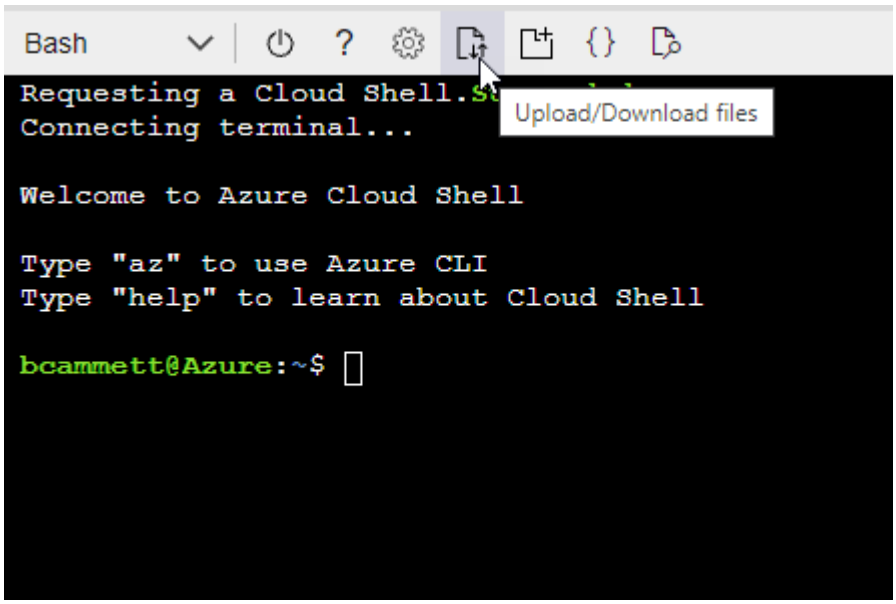
   ejemplo

```
"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:

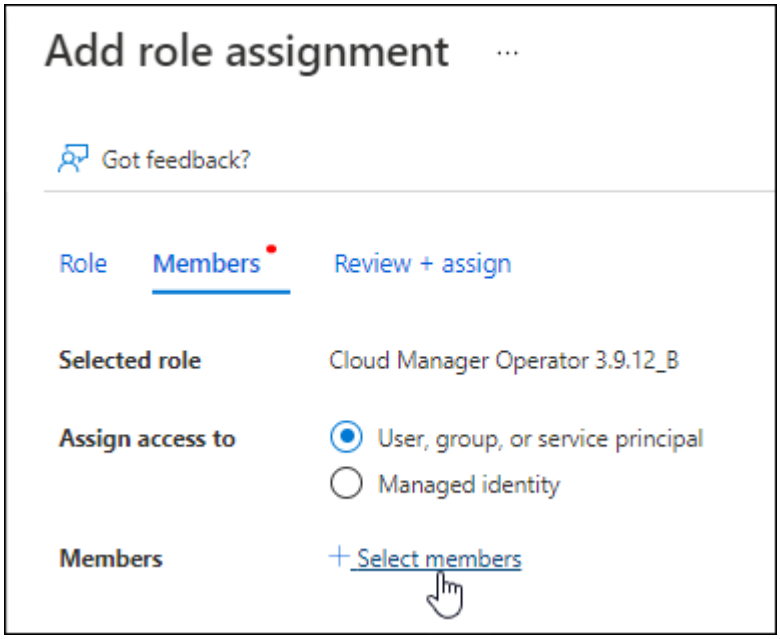
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

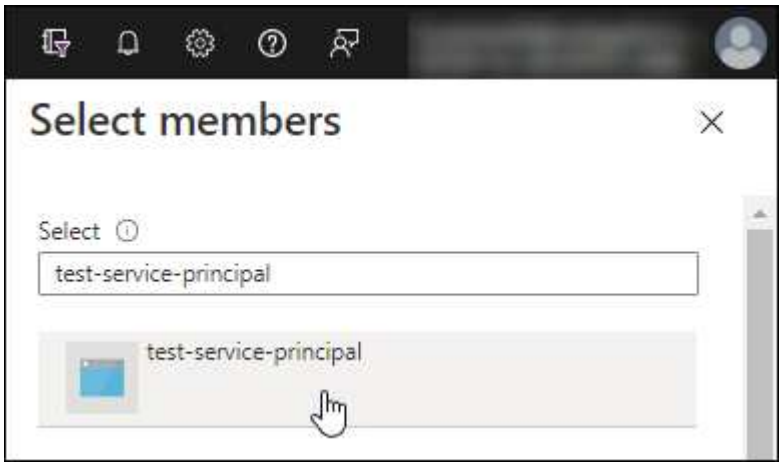
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**,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

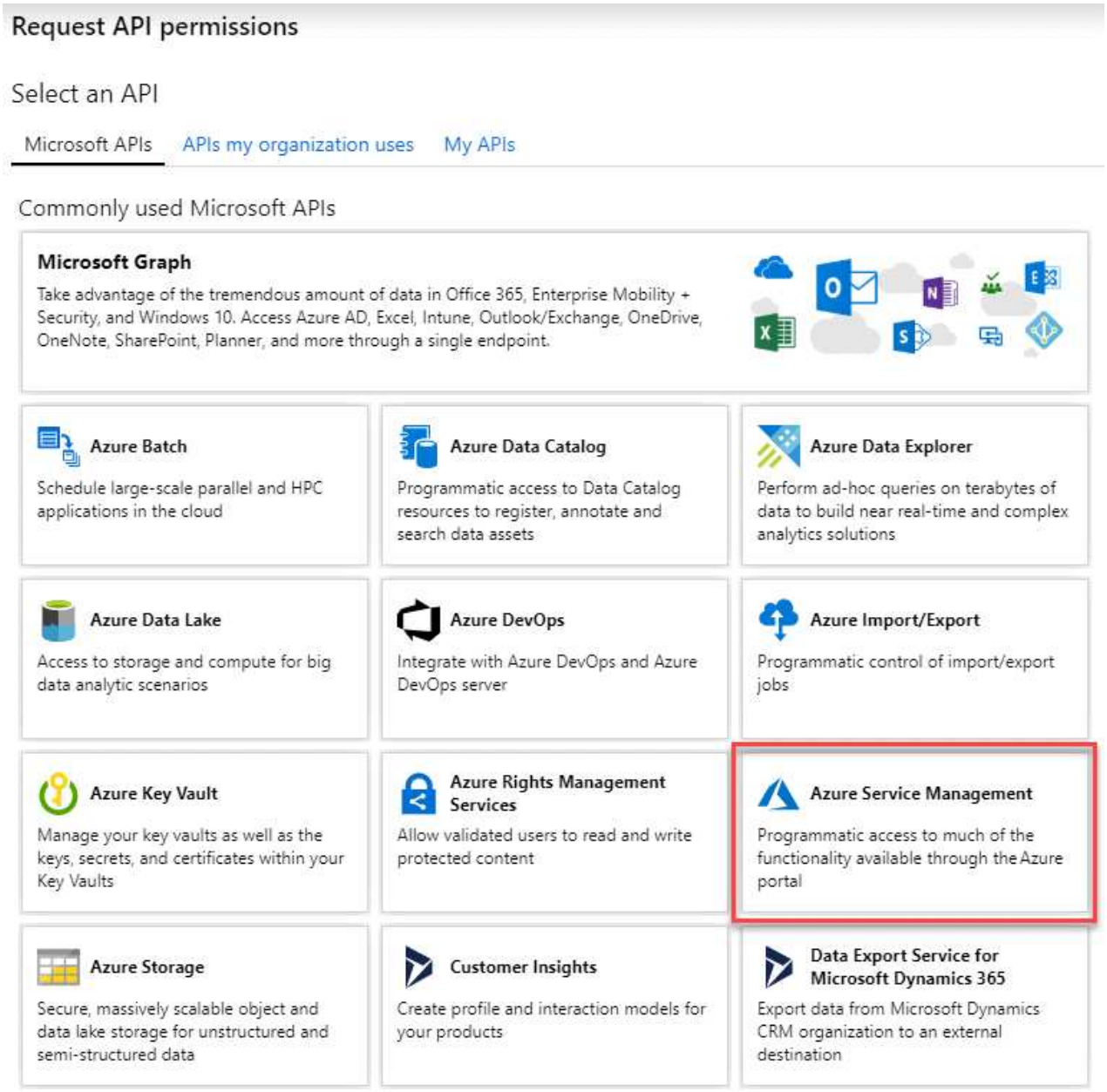
f. Seleccione **revisar + asignar**.

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

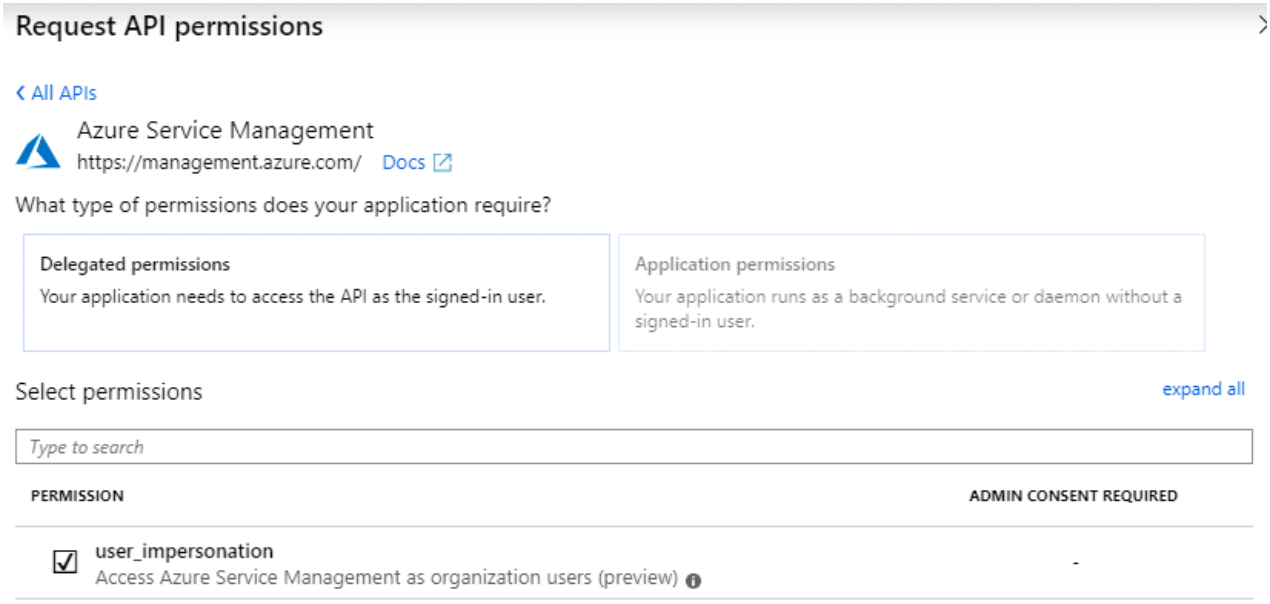
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. BlueXP le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

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**.

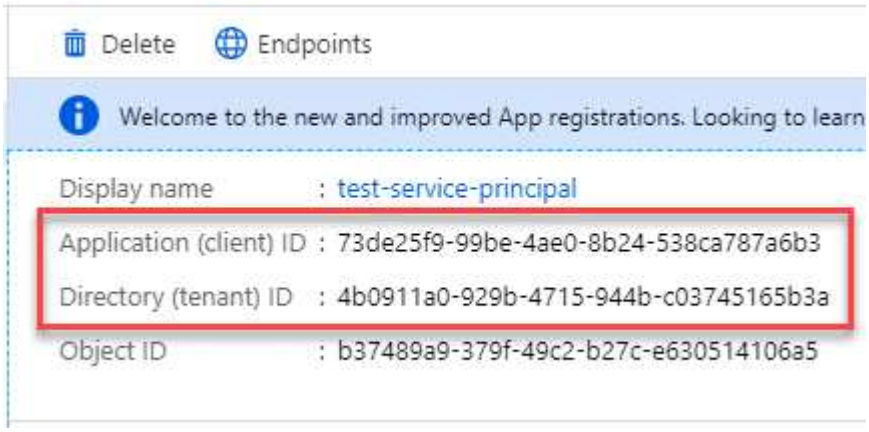


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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 5: 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.

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

  No se puede configurar un certificado para un servidor proxy transparente al instalar el Conector manualmente. Si necesita configurar un certificado para un servidor proxy transparente, debe usar la Consola de mantenimiento después de la instalación. Obtenga más información sobre el "Consola de mantenimiento del conector".

- 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. 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.

2. 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.

3. Asigne permisos para ejecutar el script.

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

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

4. 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>
```

   Necesitará agregar la información del proxy si su red requiere uno para acceder a internet. Puede agregar un proxy transparente o explícito. Los parámetros --proxy y --cacert son opcionales y no se le solicitará que los agregue. Si tiene un servidor proxy, deberá introducir los parámetros como se muestra.

   A continuación se muestra un ejemplo de configuración de un servidor proxy explícito con un certificado firmado por una CA:

```
 ./BlueXP-Connector-Cloud-v3.9.40--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 un \ como se muestra anteriormente.
- BlueXP no admite nombres de usuario ni contraseñas que incluyan el carácter @.
- Si la contraseña incluye alguno de los siguientes caracteres especiales, debe escapar de ese carácter especial preponiéndolo con una barra diagonal inversa: & O !

  Por ejemplo:

  http://bxpproxyuser:netapp1\!@address:3128

  --cacert especifica un certificado firmado por CA que se utilizará para el acceso HTTPS entre el conector y el servidor proxy. Este parámetro es necesario para servidores proxy HTTPS, servidores proxy de interceptación y servidores proxy transparentes.

A continuación se muestra un ejemplo de configuración de un servidor proxy transparente. Al configurar un proxy transparente, no es necesario definir el servidor proxy. Solo se agrega un certificado firmado por una CA al host del conector:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. Si usó Podman, necesitará ajustar el puerto aardvark-dns.
   a. SSH a la máquina virtual del conector BlueXP.
   b. Abra el archivo podman */usr/share/containers/containers.conf* y modifique el puerto seleccionado para el servicio DNS de Aardvark. Por ejemplo, cámbielo a 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. Reinicie la máquina virtual del conector.
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 organización 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**.

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 6: 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.

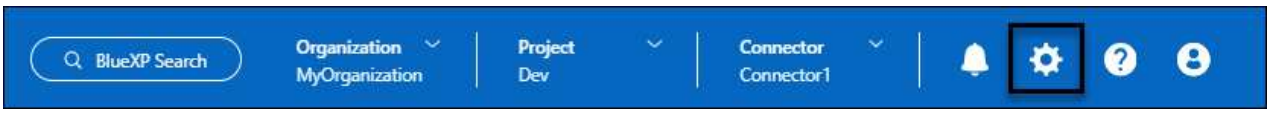
El futuro

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

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

Antes de empezar

- Usted debe tener un "Comprensión de los conectores".
- Usted debe revisar "Limitaciones del conector".

Paso 1: Configurar redes

Configure la red para garantizar que el conector pueda administrar recursos, con conexiones a redes de destino y acceso a Internet saliente.

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.

Puntos finales	Específico
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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"

Implemente 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:

```
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"

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.

Es su responsabilidad actualizar el rol personalizado a medida que se agregan nuevos permisos en las versiones posteriores. Si se requieren nuevos permisos, se mostrarán en las notas de la versión.

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

Debe habilitar varias API de Google Cloud antes de implementar Connector y Cloud Volumes ONTAP.

Paso

1. Habilite las siguientes API de Google Cloud en su proyecto:
   - API de Cloud Deployment Manager V2
   - API de registro en la nube
   - API de Cloud Resource Manager
   - API del motor de computación
   - API de gestión de acceso e identidad (IAM)
   - 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. No cambie el conector a una instancia de VM más pequeña con menos CPU o RAM después de la creación. "Obtenga información sobre la configuración predeterminada para el conector".

BlueXP

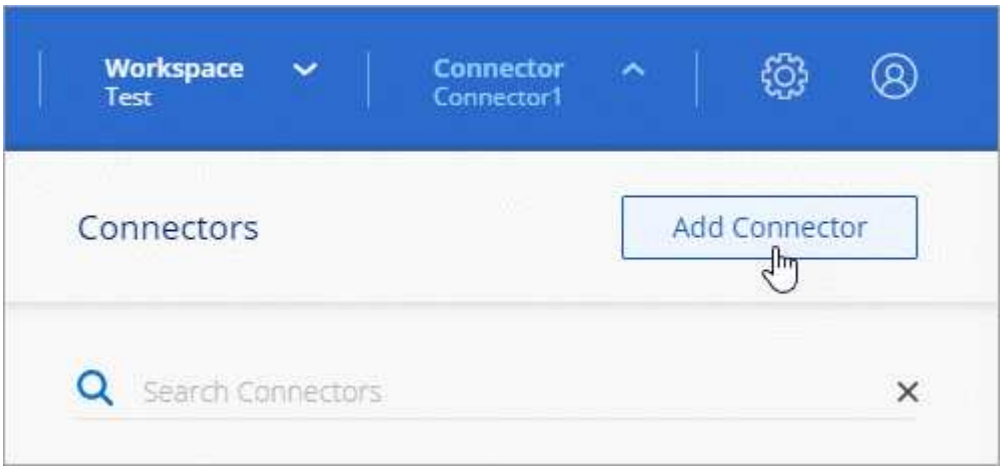
Antes de empezar

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.
   - Etiquetas de red: Si usa un proxy transparente, agregue una etiqueta de red a la instancia del Conector. Las etiquetas de red deben comenzar con minúscula y pueden contener minúsculas,

números y guiones. Deben terminar con minúscula o número. Por ejemplo, podría usar la etiqueta "connector-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 estará lista en aproximadamente 7 minutos; permanezca en la página hasta que se complete el proceso.

Resultado

Una vez completado el proceso, el conector estará disponible para su uso desde 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**: 8 núcleos o 8 vCPU
  - **RAM**: 32 GB
  - * Tipo de máquina *: Recomendamos n2-standard-8.

    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 utilizando su método preferido.

   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-8
  --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 organización BlueXP que desea asociar al conector.

      "Obtenga más información sobre la gestión de identidades y accesos de BlueXP ".

   b. Escriba un nombre para el sistema.

Resultado

El conector ya está instalado y configurado con su organización 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

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

Antes de empezar

- Usted debe tener un "Comprensión de los conectores".
- 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.

> El Conector reserva el rango de UID y GID de 19000 a 19200. Este rango es fijo y no se puede modificar. Si algún software de terceros en su host utiliza UID o GID dentro de este rango, la instalación del Conector fallará. NetApp recomienda usar un host sin software de terceros para evitar conflictos.

Host dedicado

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

Host puede ser de cualquier arquitectura que cumpla con los siguientes requisitos de tamaño:

- CPU: 8 núcleos o 8 vCPU
- RAM: 32 GB

Hipervisor

Se requiere un hipervisor nativo o alojado que esté certificado para ejecutar un sistema operativo compatible.

Requisitos del sistema operativo y del contenedor

BlueXP admite el conector con los siguientes sistemas operativos cuando se utiliza BlueXP en modo estándar o en modo restringido. Antes de instalar el conector, se necesita una herramienta de orquestación de contenedores.

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Motor Docker 23.06 a 28.0.0.	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en 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.

Tipo de máquina de Google Cloud

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos n2-standard-8.

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

BlueXP utiliza `/opt` para instalar el `/opt/application/netapp` directorio y su contenido.

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

BlueXP requiere este espacio en `/var` Porque Docker o Podman están diseñados para crear los contenedores dentro de este directorio. Específicamente, crearán contenedores en el `/var/lib/containers/storage` directorio. Los montajes externos o los enlaces simbólicos no funcionan en este espacio.

Paso 2: Instale Podman o Docker Engine

Dependiendo del sistema operativo, se requiere Podman o Docker Engine antes de instalar el conector.

- Se requiere Podman para Red Hat Enterprise Linux 8 y 9.

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 3. Pasos

Podman

Siga estos pasos para instalar Podman y configurarlo para cumplir con los siguientes requisitos:

- Habilitar e iniciar el servicio podman.socket
- Instale python3
- Instalar el paquete podman-compose versión 1.0.6
- Agregue podman-compose a la variable de entorno PATH

> Al usar Podman, ajuste el puerto del servicio aardvark-dns (predeterminado: 53) después de instalar el Conector para evitar conflictos con el puerto DNS del host. Siga las instrucciones para configurar el puerto.

Pasos

1. Elimine el paquete podman-docker si está instalado en el host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale Podman.

   Podman está disponible en repositorios oficiales de Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

3. Active e inicie el servicio podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale el paquete de repositorio de EPEL si aún no está disponible en su sistema.

   Este paso es necesario porque podman-compose está disponible en el repositorio Extra Packages for Enterprise Linux (EPEL).

   Para Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Instale el paquete podman-compose 1,0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   Con el `dnf install` El comando cumple con los requisitos para agregar podman-compose a la variable de entorno PATH. El comando installation agrega podman-compose a /usr/bin, que ya está incluido en el `secure_path` opción en el host.

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

   Asegúrese de seguir los pasos para instalar una versión específica de Docker Engine. Al instalar la versión más reciente se instalará una versión de Docker no compatible con BlueXP.

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 3: 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 desde los equipos cuando se utiliza la consola basada en web de BlueXP

Los equipos que acceden a la consola de BlueXP desde un navegador web deben tener la capacidad de contactar con varios puntos finales. Necesitará utilizar la consola BlueXP para configurar el conector y para utilizar el día a día de BlueXP .

"Prepare las redes para la consola de BlueXP ".

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://mysupport.netapp.com
- https://signin.b2c.NetApp.com (este punto final es la URL de CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- Para obtener imágenes, el instalador necesita acceder a uno de estos dos conjuntos de puntos finales:
  - Opción 1 (recomendado):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Opción 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

    Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

  - Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
  - El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
  - Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar

los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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.
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.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No

hay compatibilidad con versiones anteriores del conector.

- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Servidor proxy

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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 4: 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.

Es su responsabilidad actualizar el rol personalizado a medida que se agregan nuevos permisos en las versiones posteriores. Si se requieren nuevos permisos, se mostrarán en las notas de la versión.

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 5: 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 6: 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 7: 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.

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

> No se puede configurar un certificado para un servidor proxy transparente al instalar el Conector manualmente. Si necesita configurar un certificado para un servidor proxy transparente, debe usar la Consola de mantenimiento después de la instalación. Obtenga más información sobre el "Consola de mantenimiento del conector".

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. 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.

2. 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.

3. Asigne permisos para ejecutar el script.

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

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

4. 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>
   ```

   Necesitará agregar la información del proxy si su red requiere uno para acceder a internet. Puede agregar un proxy transparente o explícito. Los parámetros --proxy y --cacert son opcionales y no se le solicitará que los agregue. Si tiene un servidor proxy, deberá introducir los parámetros como se muestra.

   A continuación se muestra un ejemplo de configuración de un servidor proxy explícito con un certificado firmado por una CA:

   ```
    ./BlueXP-Connector-Cloud-v3.9.40--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 un \ como se muestra anteriormente.
- BlueXP no admite nombres de usuario ni contraseñas que incluyan el carácter @.
- Si la contraseña incluye alguno de los siguientes caracteres especiales, debe escapar de ese carácter especial preponiéndolo con una barra diagonal inversa: & O !

  Por ejemplo:

  http://bxpproxyuser:netapp1\!@address:3128

  --cacert especifica un certificado firmado por CA que se utilizará para el acceso HTTPS entre el conector y el servidor proxy. Este parámetro es necesario para servidores proxy HTTPS, servidores proxy de interceptación y servidores proxy transparentes.

A continuación se muestra un ejemplo de configuración de un servidor proxy transparente. Al configurar un proxy transparente, no es necesario definir el servidor proxy. Solo se agrega un certificado firmado por una CA al host del conector:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. Si usó Podman, necesitará ajustar el puerto aardvark-dns.
   a. SSH a la máquina virtual del conector BlueXP.
   b. Abra el archivo podman */usr/share/containers/containers.conf* y modifique el puerto seleccionado para el servicio DNS de Aardvark. Por ejemplo, cámbielo a 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. Reinicie la máquina virtual del conector.
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 organización 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**.

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 8: 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.

Instale y configure un conector en las instalaciones

Puede instalar un conector en una de sus máquinas locales. Para ejecutar Connector en las instalaciones, debe revisar los requisitos del host, configurar la red, preparar los permisos de la nube, instalar Connector, configurar Connector y, a continuación, proporcionar los permisos que preparó.

Antes de empezar

- Revisar información sobre "Conectores" .
- Usted debe revisar "Limitaciones del conector".

Paso 1: Revise los requisitos del host

Ejecute el software Connector en un host que cumpla con los requisitos de sistema operativo, RAM y puerto. Asegúrese de que el host cumple estos requisitos antes de instalar el conector.

> El Conector reserva el rango de UID y GID de 19000 a 19200. Este rango es fijo y no se puede modificar. Si algún software de terceros en su host utiliza UID o GID dentro de este rango, la instalación del Conector fallará. NetApp recomienda usar un host sin software de terceros para evitar conflictos.

Host dedicado

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

Host puede ser de cualquier arquitectura que cumpla con los siguientes requisitos de tamaño:

- CPU: 8 núcleos o 8 vCPU
- RAM: 32 GB

Hipervisor

Se requiere un hipervisor nativo o alojado que esté certificado para ejecutar un sistema operativo compatible.

Requisitos del sistema operativo y del contenedor

BlueXP admite el conector con los siguientes sistemas operativos cuando se utiliza BlueXP en modo estándar o en modo restringido. Antes de instalar el conector, se necesita una herramienta de orquestación de contenedores.

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Motor Docker 23.06 a 28.0.0.	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en 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.

Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

BlueXP utiliza `/opt` para instalar el `/opt/application/netapp` directorio y su contenido.

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

BlueXP requiere este espacio en `/var` Porque Docker o Podman están diseñados para crear los contenedores dentro de este directorio. Específicamente, crearán contenedores en el `/var/lib/containers/storage` directorio. Los montajes externos o los enlaces simbólicos no funcionan en este espacio.

Paso 2: Instale Podman o Docker Engine

Dependiendo del sistema operativo, se requiere Podman o Docker Engine antes de instalar el conector.

- Se requiere Podman para Red Hat Enterprise Linux 8 y 9.

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 4. Pasos

Podman

Siga estos pasos para instalar Podman y configurarlo para cumplir con los siguientes requisitos:

- Habilitar e iniciar el servicio podman.socket
- Instale python3
- Instalar el paquete podman-compose versión 1.0.6
- Agregue podman-compose a la variable de entorno PATH

> Al usar Podman, ajuste el puerto del servicio aardvark-dns (predeterminado: 53) después de instalar el Conector para evitar conflictos con el puerto DNS del host. Siga las instrucciones para configurar el puerto.

Pasos

1. Elimine el paquete podman-docker si está instalado en el host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale Podman.

   Podman está disponible en repositorios oficiales de Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

3. Active e inicie el servicio podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale el paquete de repositorio de EPEL si aún no está disponible en su sistema.

   Este paso es necesario porque podman-compose está disponible en el repositorio Extra Packages for Enterprise Linux (EPEL).

   Para Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Instale el paquete podman-compose 1,0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   Con el `dnf install` El comando cumple con los requisitos para agregar podman-compose a la variable de entorno PATH. El comando installation agrega podman-compose a /usr/bin, que ya está incluido en el `secure_path` opción en el host.

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

   Asegúrese de seguir los pasos para instalar una versión específica de Docker Engine. Al instalar la versión más reciente se instalará una versión de Docker no compatible con BlueXP.

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 3: Configurar redes

Configure la red para garantizar que el conector pueda administrar recursos, con conexiones a redes de destino y acceso a Internet saliente.

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 los equipos cuando se utiliza la consola basada en web de BlueXP

Los equipos que acceden a la consola de BlueXP desde un navegador web deben tener la capacidad de contactar con varios puntos finales. Necesitará utilizar la consola BlueXP para configurar el conector y para utilizar el día a día de BlueXP .

"Prepare las redes para la consola de BlueXP ".

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://mysupport.netapp.com
- https://signin.b2c.NetApp.com (este punto final es la URL de CNAME para https://mysupport.NetApp.com)
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- Para obtener imágenes, el instalador necesita acceder a uno de estos dos conjuntos de puntos finales:
  - Opción 1 (recomendado):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Opción 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

    Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

  - Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
  - El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
  - Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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.

Puntos finales	Específico
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Servidor proxy

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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 4: 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. Debes instalar el Conector en Google Cloud para administrar cualquier recurso que resida allí.

AWS

Cuando el conector se instala en las instalaciones, debe proporcionar a BlueXP permisos de 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, asocie estas credenciales con el Conector de BlueXP.

Azure

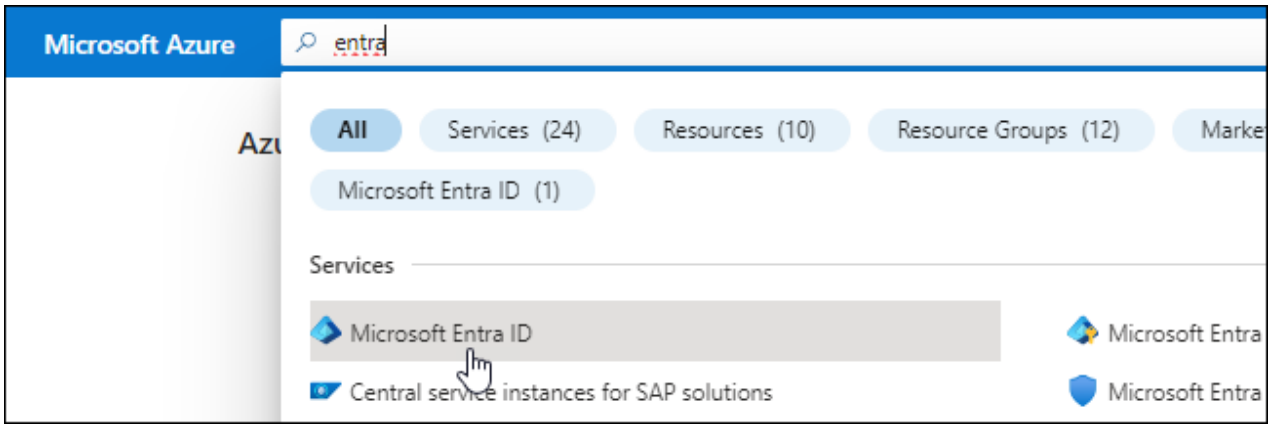
Cuando el conector se instala en las instalaciones, debe proporcionar a BlueXP permisos de Azure configurando un principal de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que BlueXP necesita.

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.

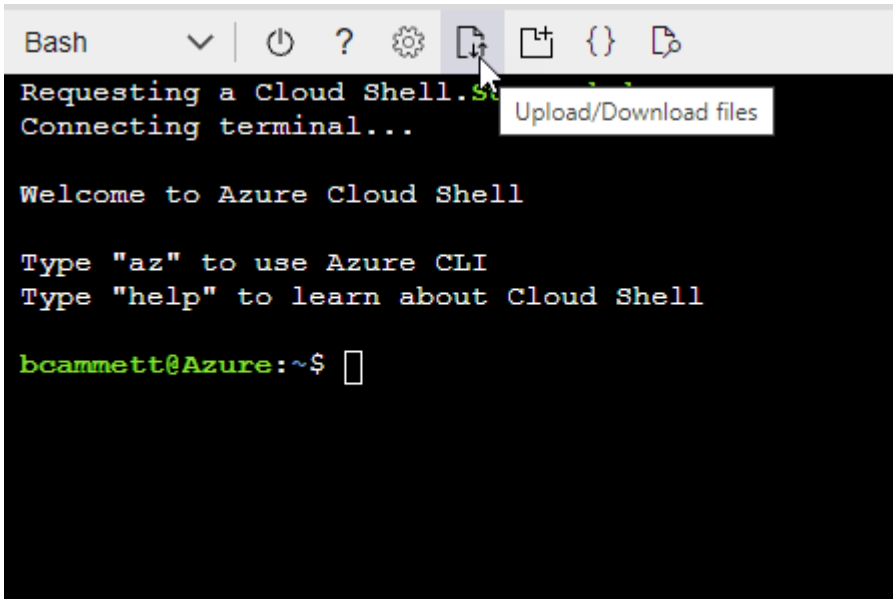
      ejemplo

```
"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**.

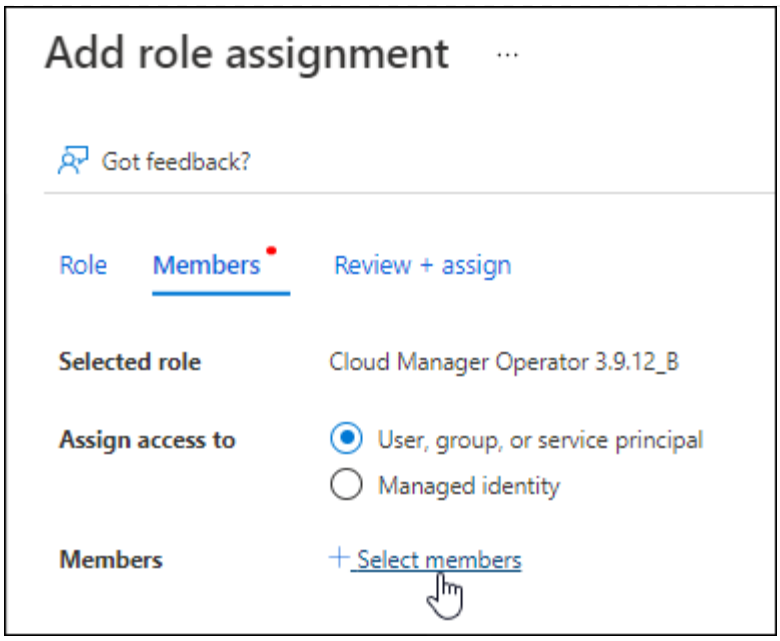
   b. Seleccione la suscripción.

   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**.

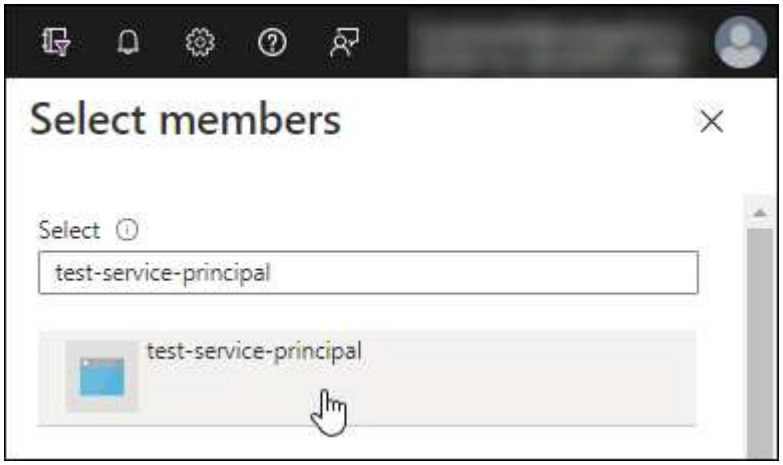
   e. En la ficha **Miembros**, realice los siguientes pasos:

      - 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**.

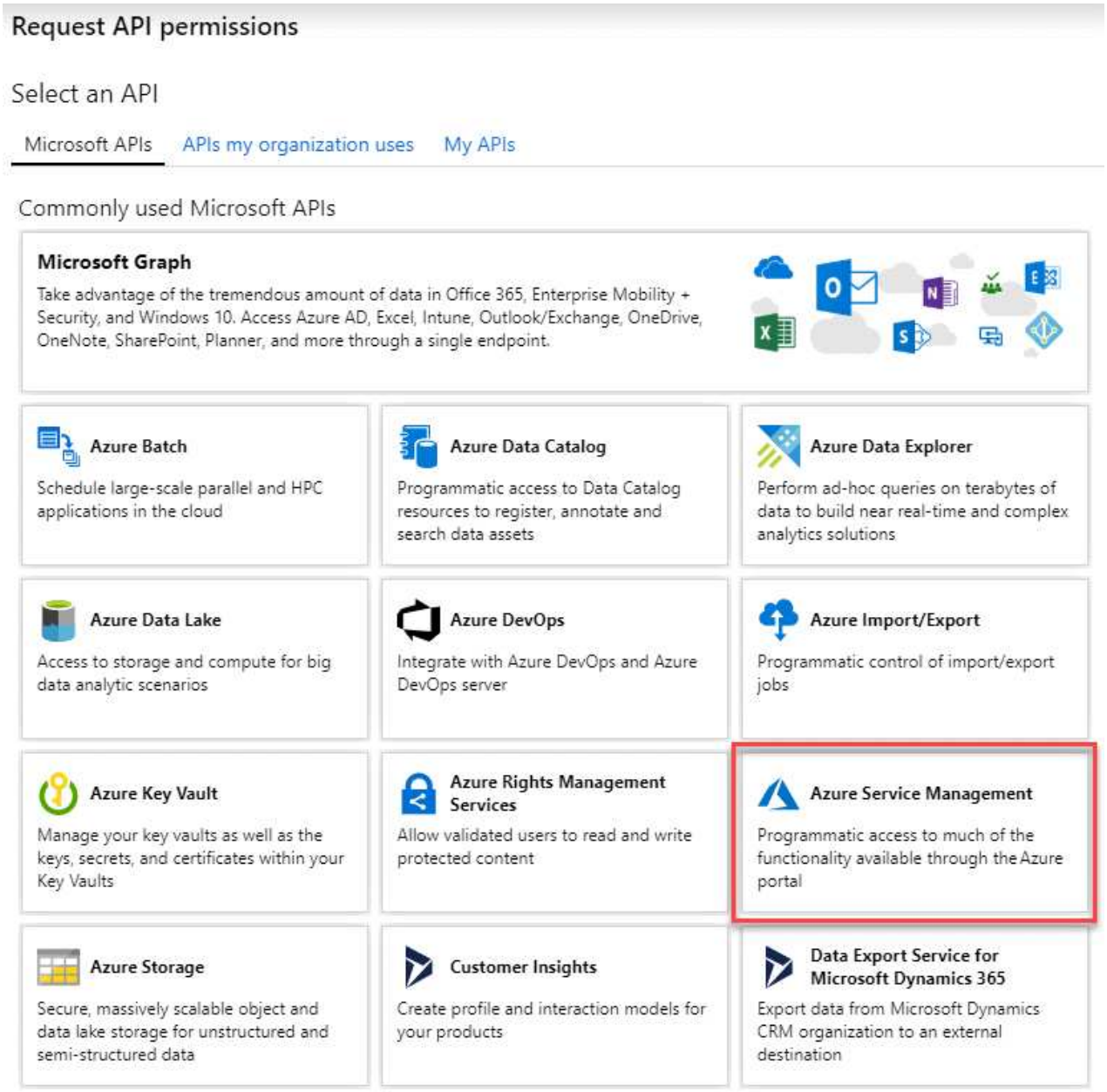
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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.

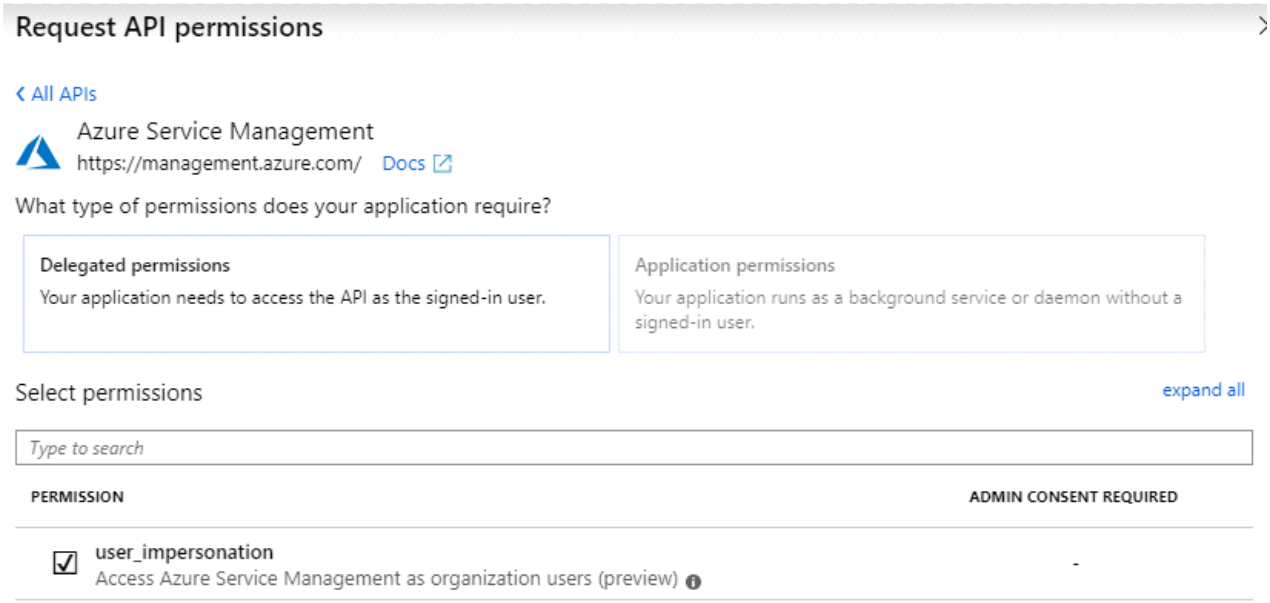
Añada permisos de API de administración de servicios de Windows Azure

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**.

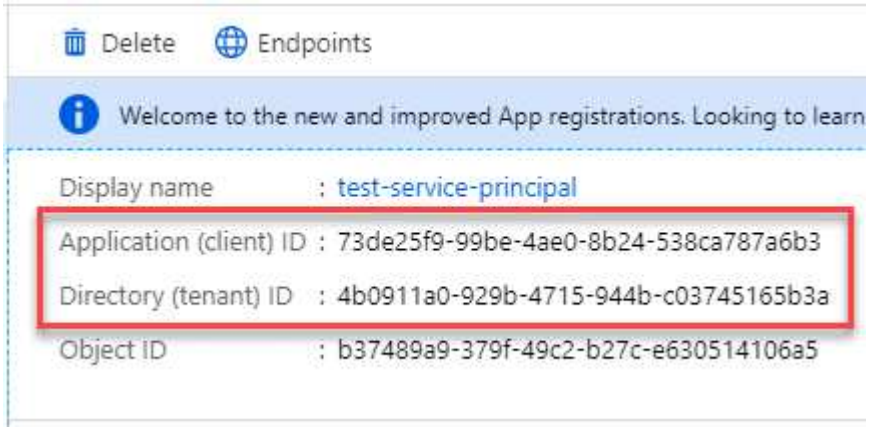


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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

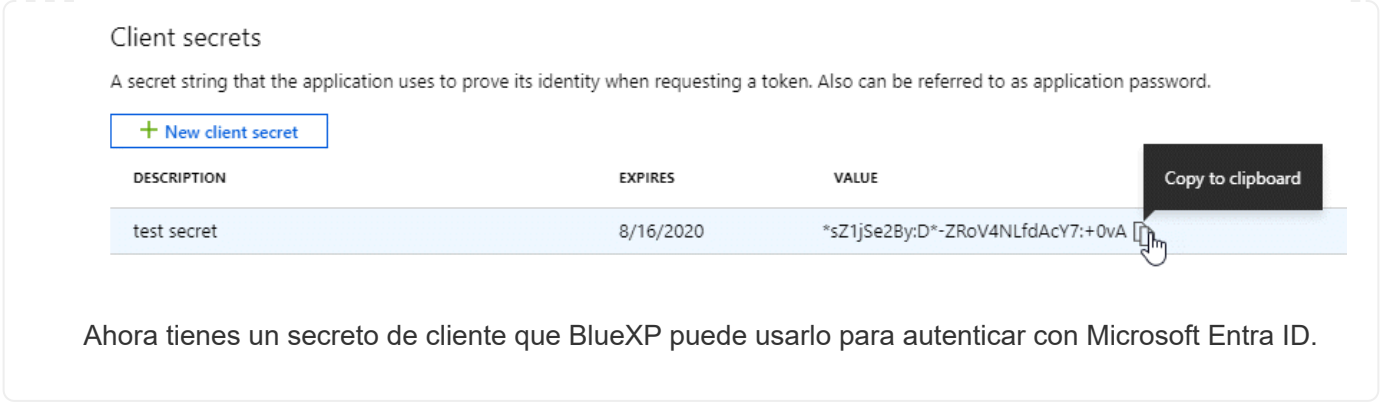
1. En el servicio **Microsoft Entra ID**, selecciona **Registros de aplicaciones** y selecciona la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



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.

Paso 5: Instale el conector

Descargue e instale el software Connector en un host Linux existente en las instalaciones.

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.

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

> No se puede configurar un certificado para un servidor proxy transparente al instalar el Conector manualmente. Si necesita configurar un certificado para un servidor proxy transparente, debe usar la Consola de mantenimiento después de la instalación. Obtenga más información sobre el "Consola de mantenimiento del conector".

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. 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.

2. 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.

3. Asigne permisos para ejecutar el script.

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

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

4. 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>
```

Necesitará agregar la información del proxy si su red requiere uno para acceder a internet. Puede agregar un proxy transparente o explícito. Los parámetros --proxy y --cacert son opcionales y no se le solicitará que los agregue. Si tiene un servidor proxy, deberá introducir los parámetros como se muestra.

A continuación se muestra un ejemplo de configuración de un servidor proxy explícito con un certificado firmado por una CA:

```
 ./BlueXP-Connector-Cloud-v3.9.40--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 un \ como se muestra anteriormente.
  - BlueXP no admite nombres de usuario ni contraseñas que incluyan el carácter @.
  - Si la contraseña incluye alguno de los siguientes caracteres especiales, debe escapar de ese carácter especial preponiéndolo con una barra diagonal inversa: & O !

    Por ejemplo:

    http://bxpproxyuser:netapp1\!@address:3128

--cacert especifica un certificado firmado por CA que se utilizará para el acceso HTTPS entre el conector y el servidor proxy. Este parámetro es necesario para servidores proxy HTTPS, servidores proxy de interceptación y servidores proxy transparentes.

A continuación se muestra un ejemplo de configuración de un servidor proxy transparente. Al configurar un proxy transparente, no es necesario definir el servidor proxy. Solo se agrega un certificado firmado por una CA al host del conector:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. Si usó Podman, necesitará ajustar el puerto aardvark-dns.
   a. SSH a la máquina virtual del conector BlueXP.
   b. Abra el archivo podman */usr/share/containers/containers.conf* y modifique el puerto seleccionado para el servicio DNS de Aardvark. Por ejemplo, cámbielo a 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. Reinicie la máquina virtual del conector.

Resultado

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

Paso 6: Registre el conector con BlueXP

Inicie sesión en BlueXP y asocie el Conector a su organización. El inicio de sesión depende del modo en que utilice BlueXP. Si utiliza BlueXP en modo estándar, inicie sesión a través del sitio web de SaaS. Si utiliza BlueXP en modo restringido o privado, inicie sesión localmente desde el host del Conector.

Pasos

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

   https://ipaddress

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

2. Regístrese o inicie sesión.
3. Después de iniciar sesión, configure BlueXP:
    a. Especifique la organización 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.

        Mantenga el modo restringido deshabilitado porque estos pasos utilizan BlueXP en modo estándar. (Además, el modo restringido no es compatible cuando el conector está instalado en las instalaciones).

    d. Selecciona **Comenzar**.

Paso 7: 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.

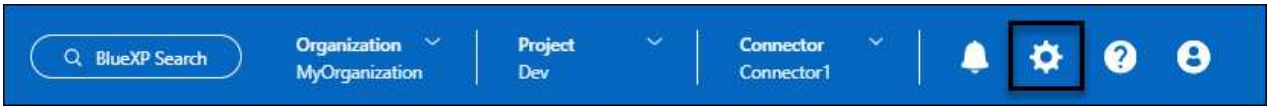
AWS

Antes de empezar

Si acaba de crear estas credenciales de AWS, es posible que tarden unos minutos en estar disponibles. 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.

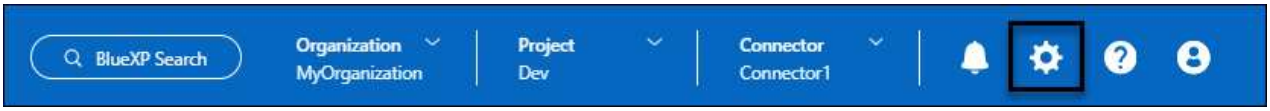
Azure

Antes de empezar

Si acaba de crear estas credenciales de Azure, es posible que tarden unos minutos en estar disponibles. 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.

Suscríbase a NetApp Intelligent Services (modo estándar)

Suscríbete a NetApp Intelligent Services desde el marketplace de tu proveedor de nube para pagar los servicios de datos a una tarifa por hora (PAYGO) o mediante 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 de mercado permite cobrar por los siguientes servicios de datos de NetApp:

- Backup y recuperación
- Cloud Volumes ONTAP
- Organización en niveles
- Protección contra ransomware
- Recuperación tras siniestros

La clasificación se habilita a través de su suscripción, pero no hay ningún cargo por utilizarla.

Antes de empezar

La suscripción a servicios de datos implica asociar una suscripción de mercado con las credenciales de la nube que están 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

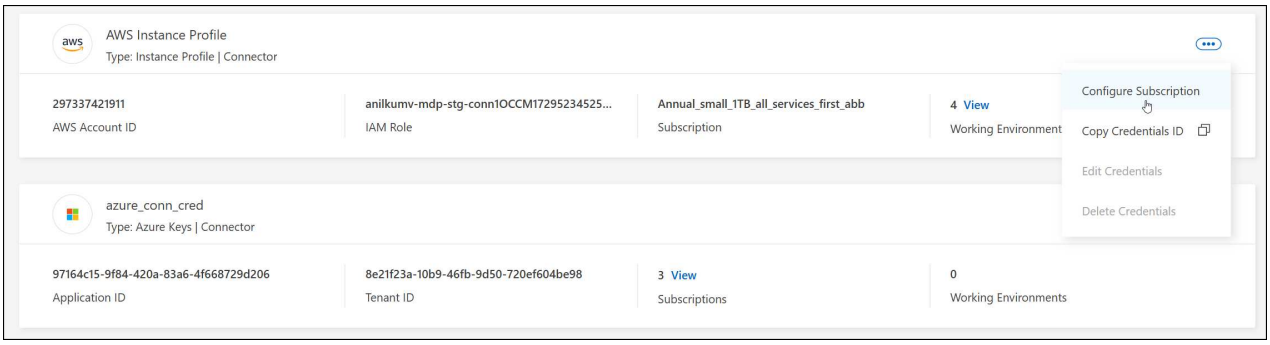
El siguiente vídeo muestra los pasos para suscribirse a NetApp Intelligent Services desde AWS Marketplace:

Suscríbase a NetApp Intelligent Services desde AWS Marketplace

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 **Configurar suscripción**.

   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 de la lista desplegable y seleccione **Configurar**.
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 organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
      - En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

        BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o 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 todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

Azure

Pasos

1. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Configurar suscripción**.

   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 de la lista desplegable y seleccione **Configurar**.
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**.

      Serás redirigido a BlueXP.

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

      - Seleccione las organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
      - En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

        BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o 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 todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

      - Seleccione **Guardar**.

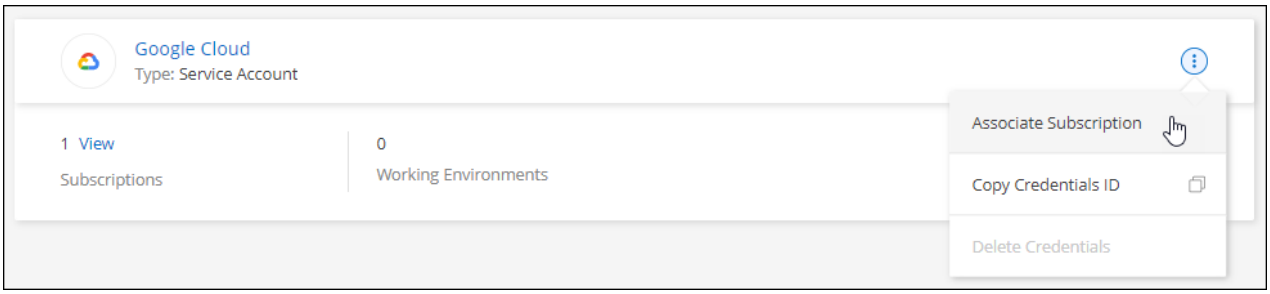
        En el siguiente vídeo se muestran los pasos para suscribirse desde Azure Marketplace:

   Suscríbase a NetApp Intelligent Services desde Azure Marketplace

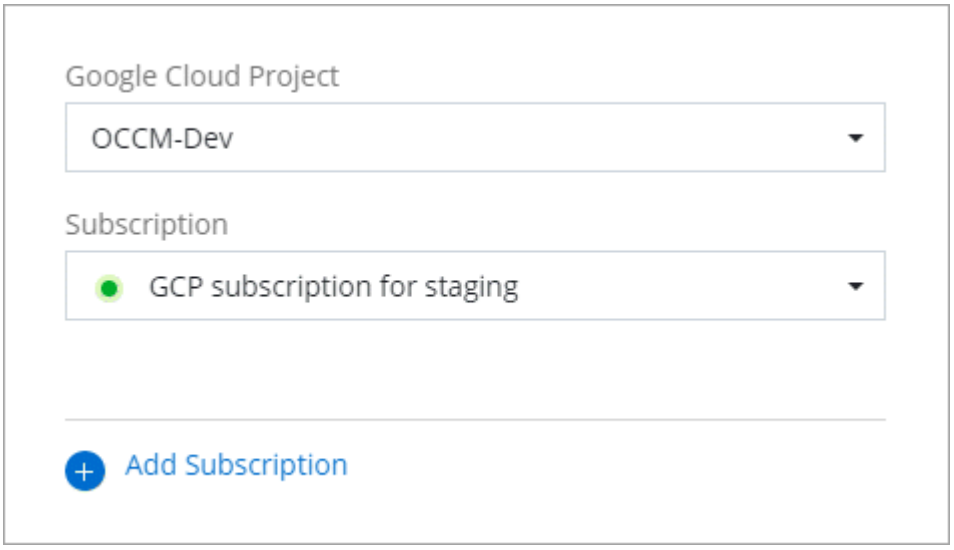
Google Cloud

Pasos

1. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Configurar suscripción**. +nueva captura de pantalla necesaria (TS)



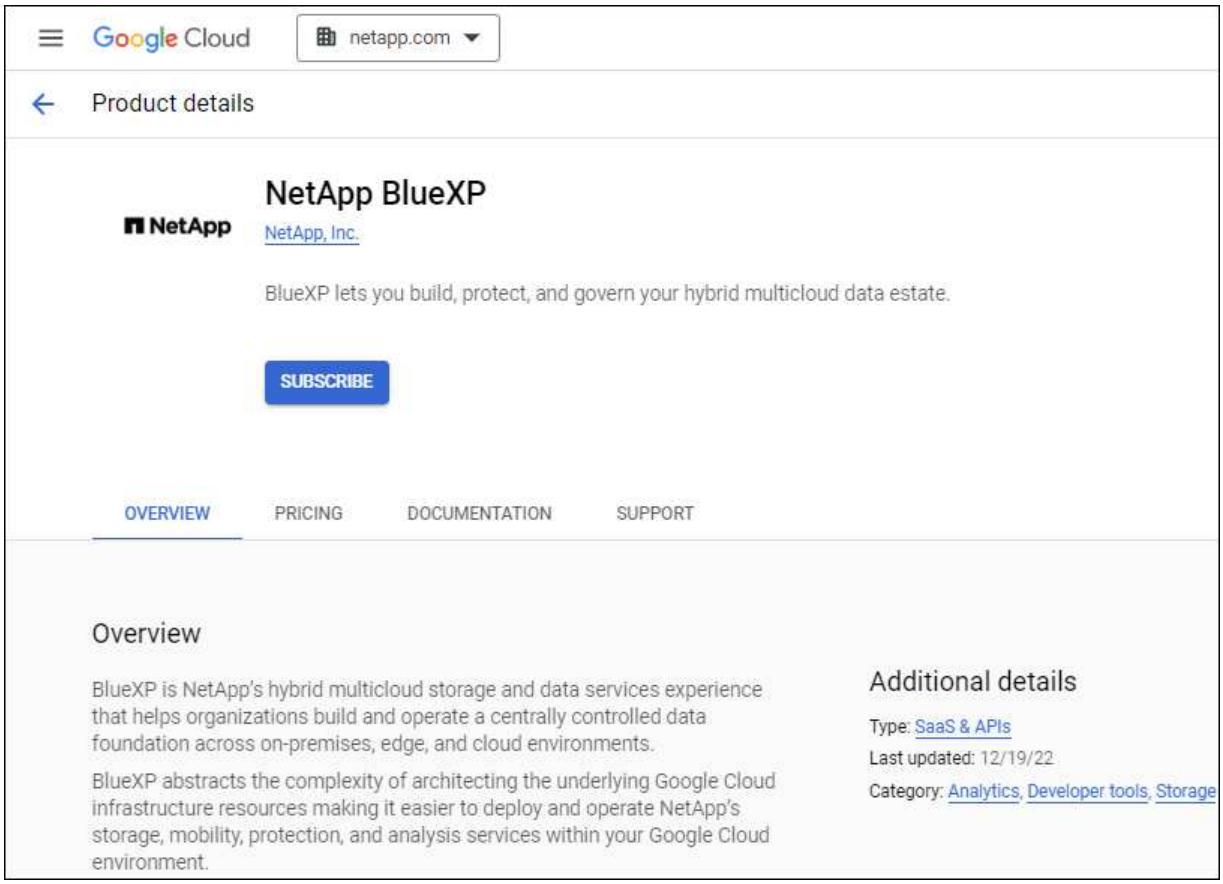
3. Para configurar una suscripción existente con las credenciales seleccionadas, seleccione un proyecto y una suscripción de Google Cloud en la lista desplegable y, a continuación, seleccione **Configurar**.



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. Después de ser redirigido a la "Página de Servicios inteligentes de NetApp en Google Cloud Marketplace" , asegúrese de que el proyecto correcto esté seleccionado en el menú de navegación superior.

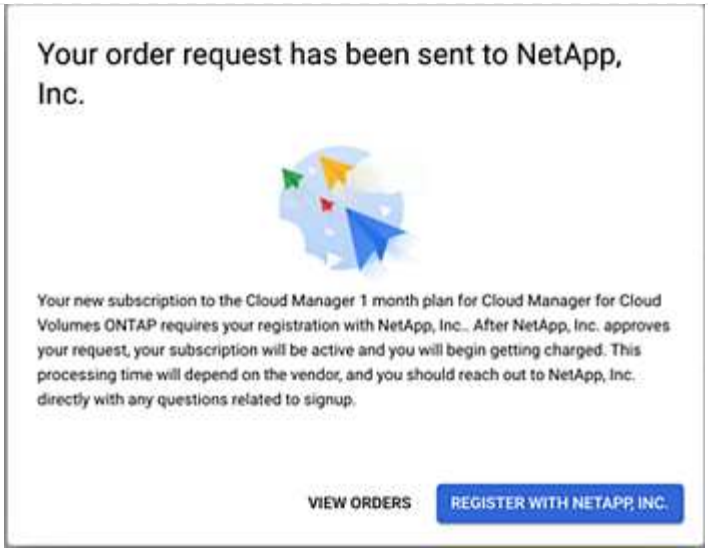


b. Seleccione **Suscribirse**.
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.
d. Seleccione **Suscribirse**.

   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 con tu organización o 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 organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
- En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

  BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o 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.

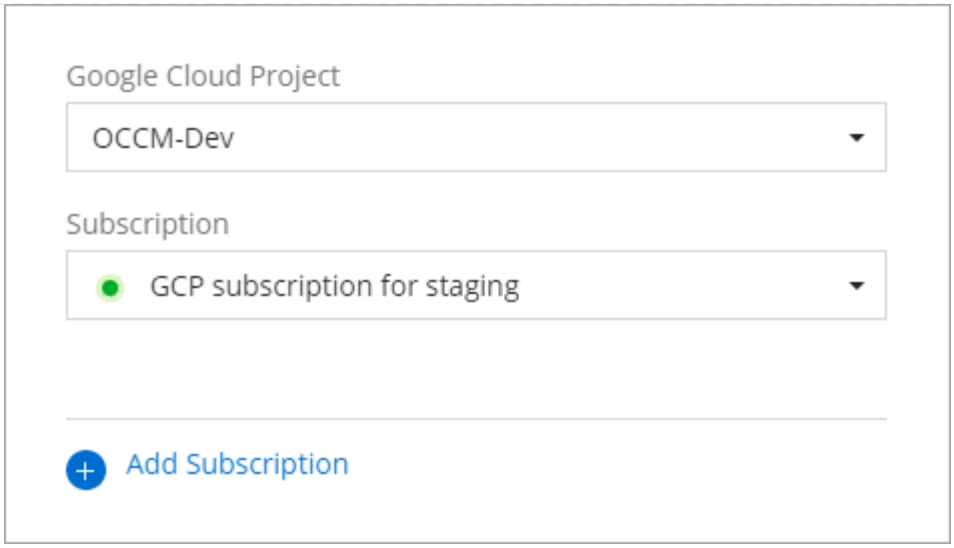
Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- 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.



Información relacionada

- "Gestione las licencias basadas en la capacidad de su propia licencia para Cloud Volumes ONTAP"
- "Administrar licencias BYOL para servicios de datos"
- "Administrar credenciales y suscripciones de AWS"
- "Administrar credenciales y suscripciones de Azure"
- "Administrar credenciales y suscripciones de Google Cloud"

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.

Información relacionada

"Modos de implementación de BlueXP"

Comience con el modo restringido

Flujo de trabajo inicial (modo restringido)

Comience a utilizar BlueXP en modo restringido preparando su entorno e implementando el Conector.

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 comenzar, asegúrese de comprender "Conectores" y "modos de despliegue" .

"Prepárese para la puesta en marcha"

1. Prepare un host Linux dedicado que cumpla con los requisitos de CPU, RAM, espacio en disco, herramienta de orquestación de contenedores y 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.

"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.

"Suscríbase a los servicios inteligentes de NetApp (opcional)"

Opcional: Suscríbase a los Servicios Inteligentes de NetApp desde el marketplace de su proveedor de nube para pagar los servicios de datos por hora (PAYGO) o mediante un contrato anual. Los Servicios Inteligentes de NetApp incluyen backup y recuperación, Cloud Volumes ONTAP, clasificación por niveles, protección contra ransomware y recuperación ante desastres. La clasificación está incluida en su suscripción sin coste adicional.

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.

Host puede ser de cualquier arquitectura que cumpla con los siguientes requisitos de tamaño:

- CPU: 8 núcleos o 8 vCPU
- RAM: 32 GB

Hipervisor

Se requiere un hipervisor nativo o alojado que esté certificado para ejecutar un sistema operativo compatible.

Requisitos del sistema operativo y del contenedor

BlueXP admite el conector con los siguientes sistemas operativos cuando se utiliza BlueXP en modo estándar o en modo restringido. Antes de instalar el conector, se necesita una herramienta de orquestación de contenedores.

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Motor Docker 23.06 a 28.0.0.	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.

3. Para RHEL, el host debe estar registrado en 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.

Tipo de instancia de AWS EC2

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos t3.2xlarge.

Tamaño de la máquina virtual de Azure

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos Standard_D8s_v3.

Tipo de máquina de Google Cloud

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos n2-standard-8.

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

BlueXP utiliza `/opt` para instalar el `/opt/application/netapp` directorio y su contenido.

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

BlueXP requiere este espacio en `/var` Porque Docker o Podman están diseñados para crear los contenedores dentro de este directorio. Específicamente, crearán contenedores en el `/var/lib/containers/storage` directorio. Los montajes externos o los enlaces simbólicos no funcionan en este espacio.

Paso 4: Instale Podman o Docker Engine

Si planea instalar manualmente el software Connector, debe preparar el host instalando Podman o Docker Engine.

Dependiendo del sistema operativo, se requiere Podman o Docker Engine antes de instalar el conector.

- Se requiere Podman para Red Hat Enterprise Linux 8 y 9.

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 5. Pasos

Podman

Siga estos pasos para instalar Podman y configurarlo para cumplir con los siguientes requisitos:

- Habilitar e iniciar el servicio podman.socket
- Instale python3
- Instalar el paquete podman-compose versión 1.0.6
- Agregue podman-compose a la variable de entorno PATH

Al usar Podman, ajuste el puerto del servicio aardvark-dns (predeterminado: 53) después de instalar el Conector para evitar conflictos con el puerto DNS del host. Siga las instrucciones para configurar el puerto.

Pasos

1. Elimine el paquete podman-docker si está instalado en el host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale Podman.

   Podman está disponible en repositorios oficiales de Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

3. Active e inicie el servicio podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale el paquete de repositorio de EPEL si aún no está disponible en su sistema.

   Este paso es necesario porque podman-compose está disponible en el repositorio Extra Packages for Enterprise Linux (EPEL).

   Para Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Instale el paquete podman-compose 1,0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   Con el `dnf install` El comando cumple con los requisitos para agregar podman-compose a la variable de entorno PATH. El comando installation agrega podman-compose a /usr/bin, que ya está incluido en el `secure_path` opción en el host.

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

   Asegúrese de seguir los pasos para instalar una versión específica de Docker Engine. Al instalar la versión más reciente se instalará una versión de Docker no compatible con BlueXP.

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 5: 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://api.bluexp.netapp.com	La consola basada en web de BlueXP se pone en contacto con este punto final para interactuar con la API de BlueXP en relación con las acciones relacionadas con la autorización, licencias, suscripciones, credenciales, notificaciones y más.
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

Cuando instala manualmente Connector en su propio host Linux, el instalador del Connector requiere acceso a varias URL durante el proceso de instalación.

- Los siguientes puntos finales siempre se contactan sin importar dónde instale el conector:
  - https://mysupport.netapp.com
  - https://signin.b2c.NetApp.com (este punto final es la URL de CNAME para https://mysupport.NetApp.com)
  - https://cloudmanager.cloud.netapp.com/tenancy
  - https://stream.cloudmanager.cloud.netapp.com
  - https://production-artifacts.cloudmanager.cloud.netapp.com
- Si instala Connector en una región de AWS Government, Installer también necesita acceso a estos puntos finales:
  - https://*.blob.core.windows.net
  - https://cloudmanagerinfraprod.azurecr.io
- Si instala Connector en una región de Azure Government, el instalador también necesita acceso a estos puntos finales:

- https://*.blob.core.windows.net
- https://occmclientinfragov.azurecr.us

- Si instala Connector en una región comercial o soberana, puede elegir entre dos conjuntos de puntos finales:
  - Opción 1 (recomendado):
    - https://bluexpinfraprod.eastus2.data.azurecr.io
    - https://bluexpinfraprod.azurecr.io
  - Opción 2:
    - https://*.blob.core.windows.net
    - https://cloudmanagerinfraprod.azurecr.io

    Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

  - Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
  - El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
  - Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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"

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.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.
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.
Si el conector se encuentra en una región gubernamental de AWS: https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector cuando Connector está instalado en una región gubernamental de AWS.
Si el conector se encuentra en una región gubernamental de Azure: https://*.blob.core.windows.net https://occmclientinfragov.azurecr.us	Para obtener imágenes para actualizaciones de Connector cuando Connector está instalado en una región de gobierno de Azure.

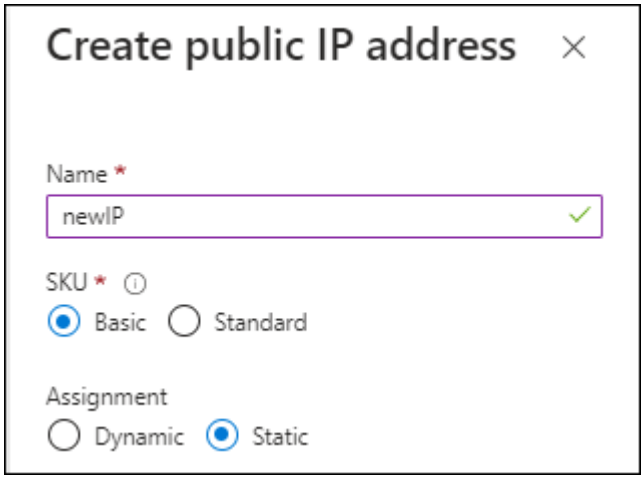
Puntos finales	Específico
Si el conector se encuentra en una región comercial o soberana, puede elegir entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector cuando Connector está instalado en una región comercial o soberana.

[1] Se recomiendan los puntos finales enumerados en la opción 1 porque son más seguros. Le recomendamos que configure su firewall para permitir los puntos finales enumerados en la opción 1, mientras no permite los puntos finales enumerados en la opción 2. Tenga en cuenta lo siguiente acerca de estos puntos finales:

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.
- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

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 6: Preparar 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.

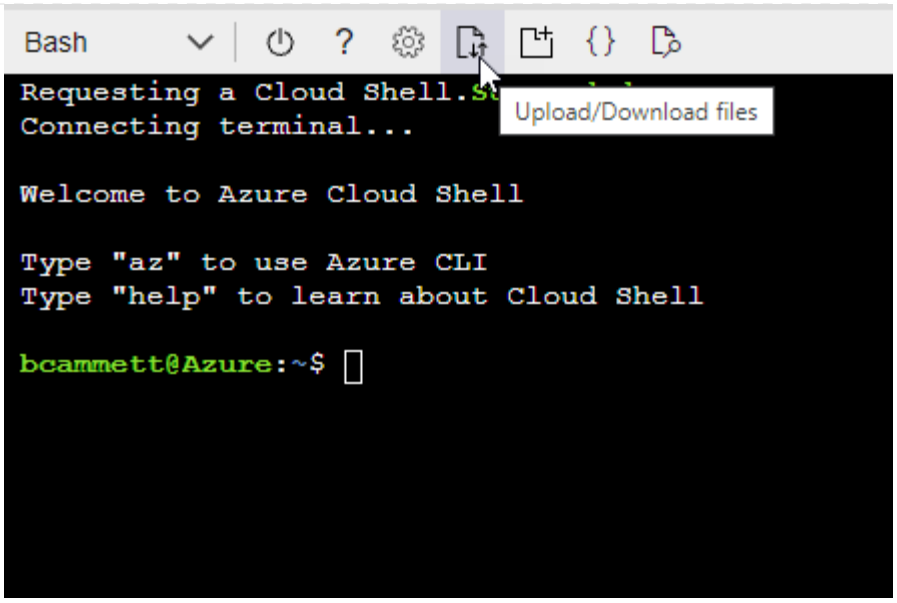
   ejemplo

   ```
   "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

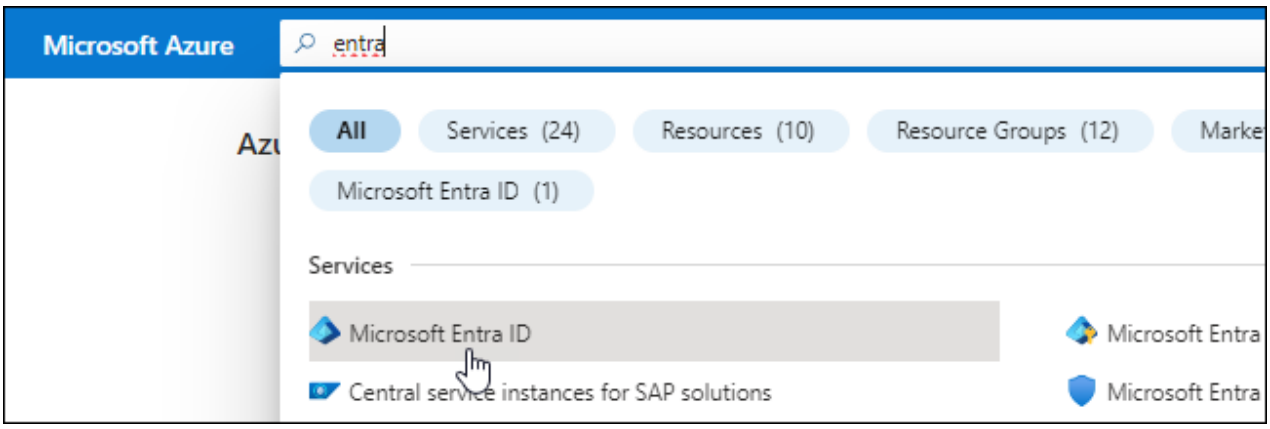
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita. Necesitará proporcionar estas credenciales a BlueXP después de instalar el conector y configurar BlueXP.

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.

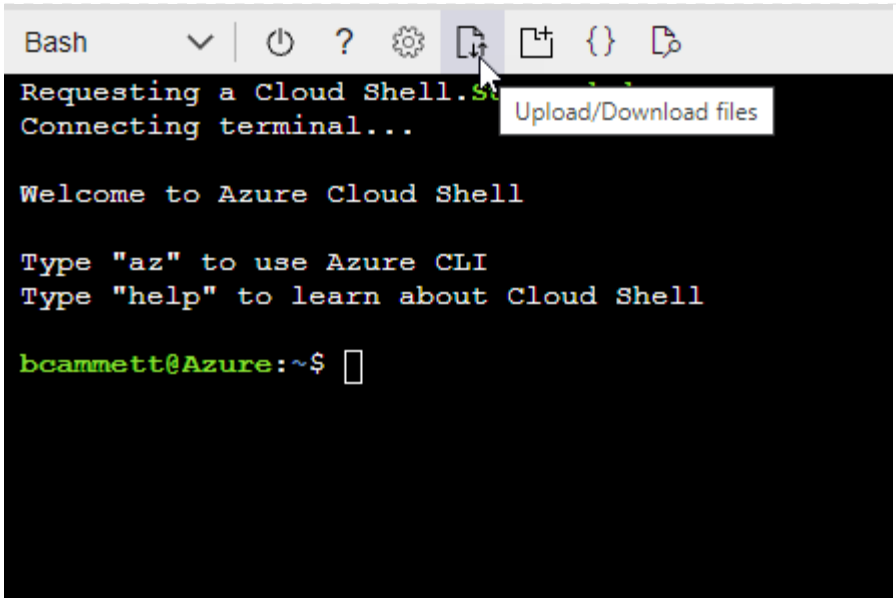
      ejemplo

      ```
      "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:

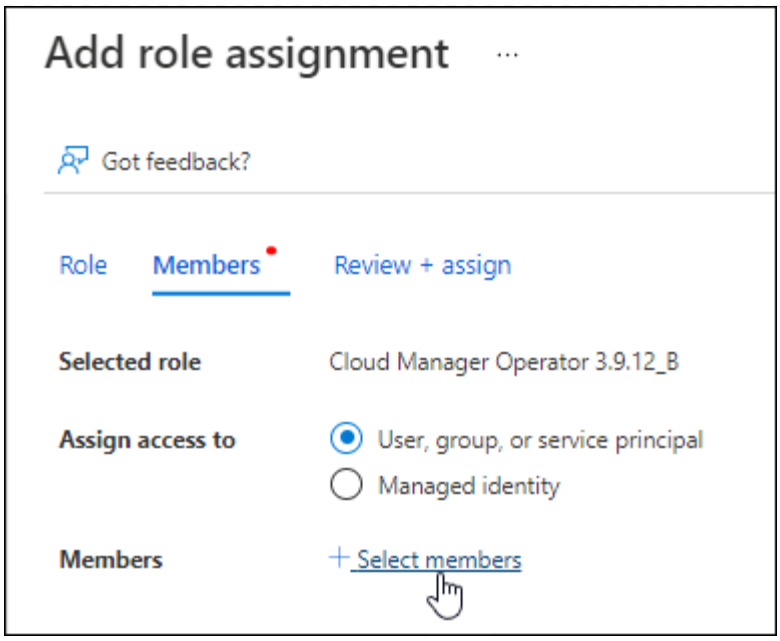
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

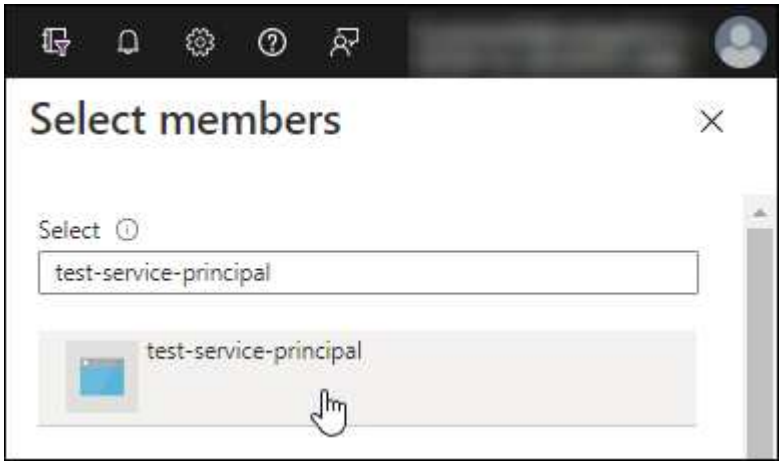
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**,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

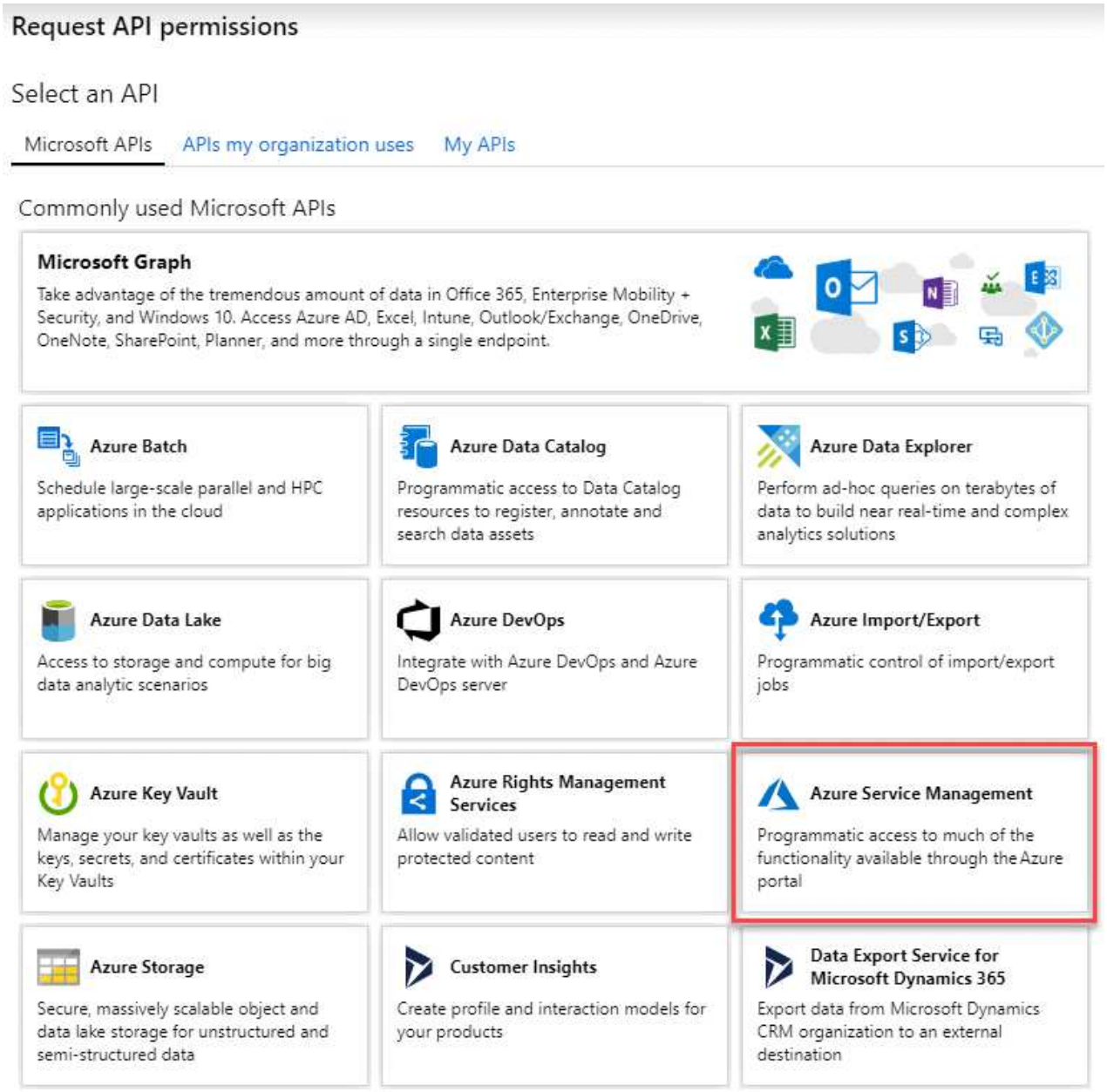
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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.

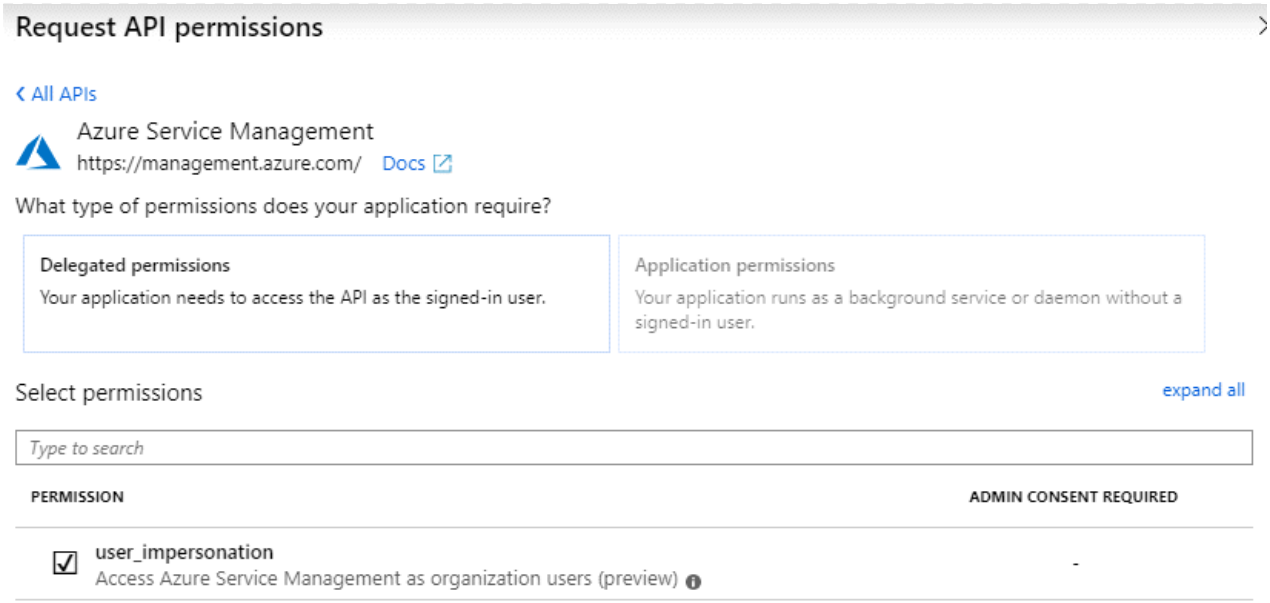
Añada permisos de API de administración de servicios de Windows Azure

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**.

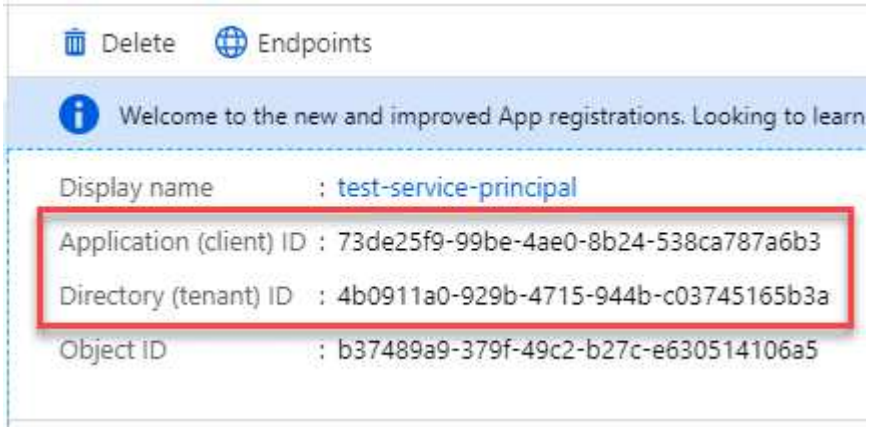


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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 7: 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

Implemente el conector en modo restringido para que pueda usar BlueXP con conectividad saliente limitada. 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"

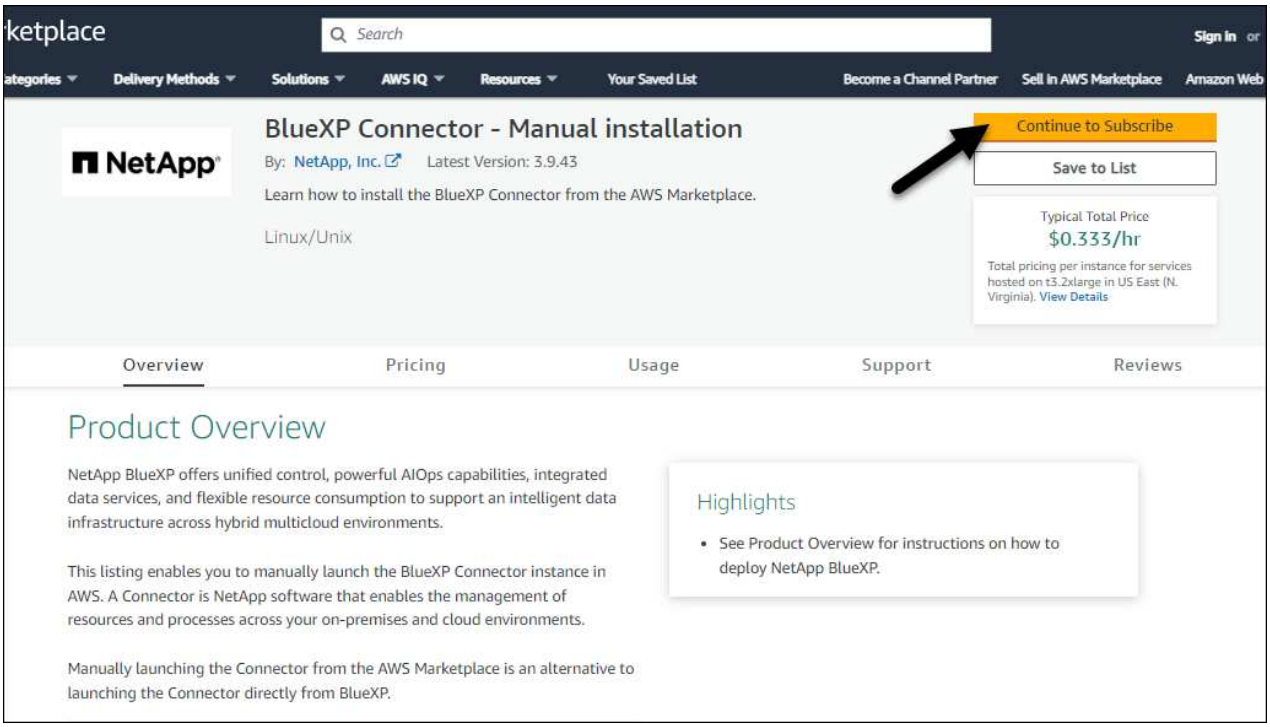
- Permisos para suscribirse y cancelar la suscripción a AWS Marketplace para su usuario de IAM.
- Comprensión de los requisitos de CPU y RAM para la instancia.

  "Revisar requisitos de instancia".

- Una pareja de claves para la instancia de EC2.

Pasos

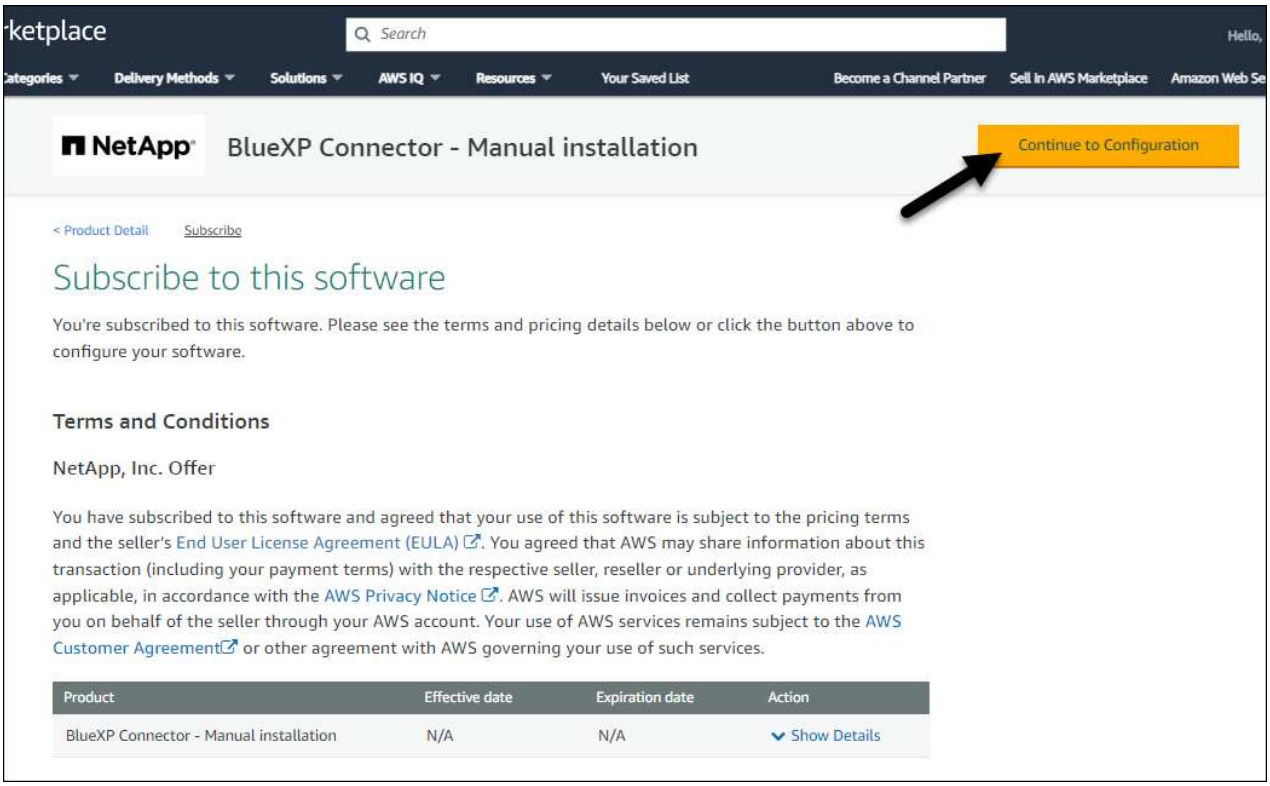
1. Vaya a la "Lista del conector BlueXP en el AWS Marketplace"
2. En la página de Marketplace, selecciona **Continuar para suscribirte**.



3. Para suscribirse al software, seleccione **Aceptar Términos**.

   El proceso de suscripción puede tardar unos minutos.

4. Una vez completado el proceso de suscripción, selecciona **Continuar con la configuración**.



5. En la página **Configurar este software**, asegúrate de haber seleccionado la región correcta y luego selecciona **Continuar para iniciar**.
6. En la página **Iniciar este software**, 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**.

7. Siga las instrucciones para configurar y desplegar la instancia:
   - **Nombre y etiquetas**: Introduzca un nombre y etiquetas para la instancia.
   - **Aplicaciones e imágenes del sistema operativo**: Omita 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 (t3,2xlarge está preseleccionado y recomendado).
   - **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 grupo de seguridad que habilite los métodos de conexión necesarios para la instancia de conector: SSH, HTTP y HTTPS.

       "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"

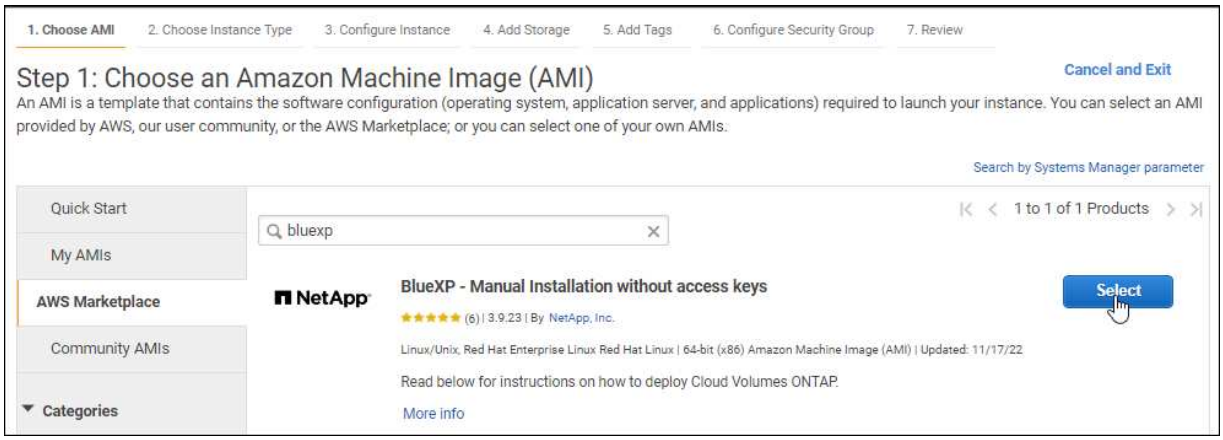
- Función IAM con una directiva adjunta que incluye los permisos necesarios para el conector.

  "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.

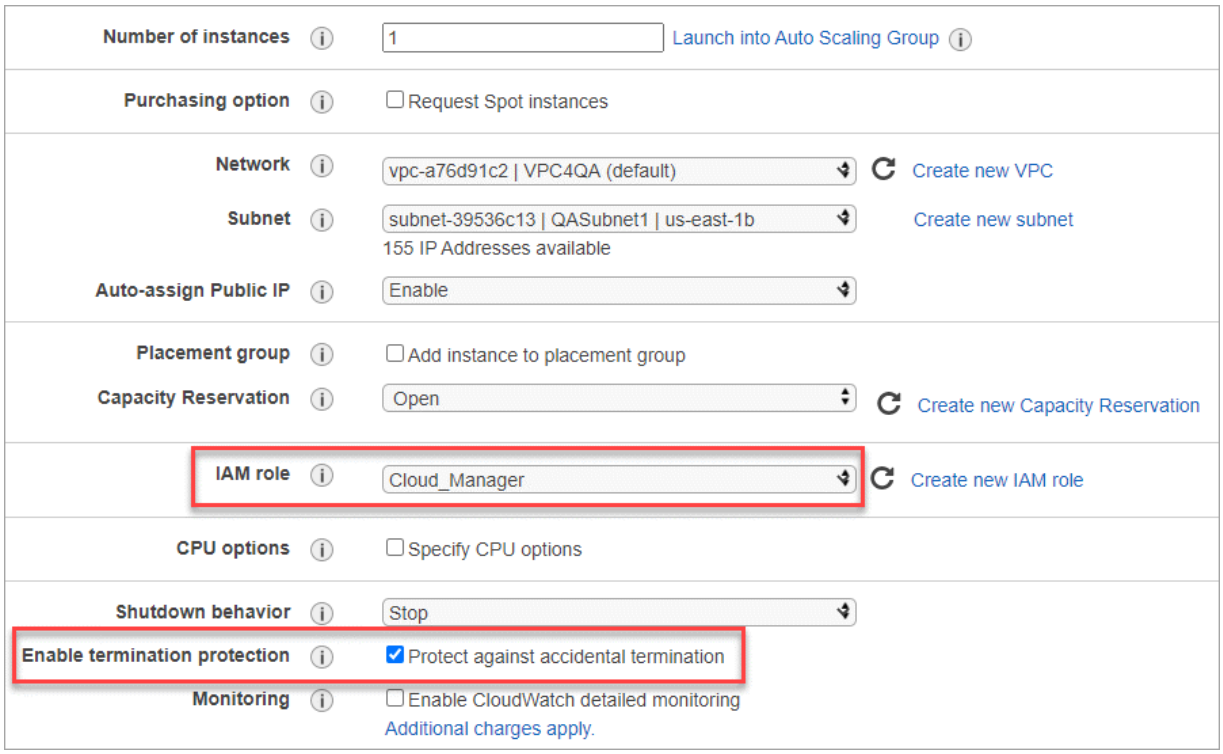


   d. Seleccione **continuar**.
2. Siga las instrucciones para configurar y desplegar la instancia:

- **Elija un tipo de instancia**: En función de la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.2xlarge).

  "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.

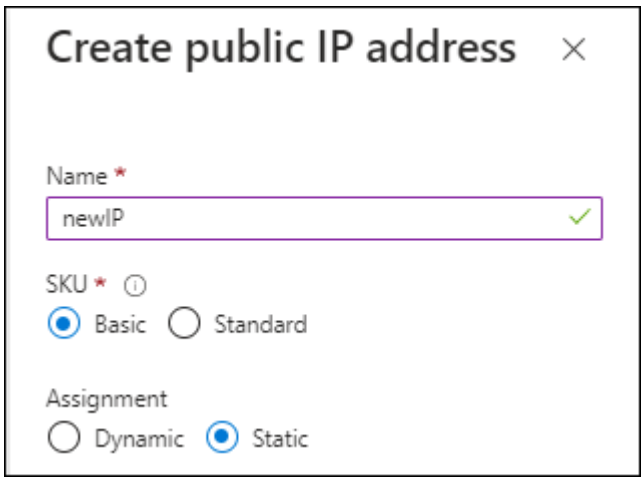
  "Aprenda a configurar los permisos de Azure"

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 Standard_D8s_v3.
   - **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.

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

> No se puede configurar un certificado para un servidor proxy transparente al instalar el Conector manualmente. Si necesita configurar un certificado para un servidor proxy transparente, debe usar la Consola de mantenimiento después de la instalación. Obtenga más información sobre el "Consola de mantenimiento del conector".

- Dependiendo del sistema operativo, se requiere Podman o Docker Engine antes de instalar el conector.

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. 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.

2. 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.

3. Asigne permisos para ejecutar el script.

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

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

4. 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>
```

Necesitará agregar la información del proxy si su red requiere uno para acceder a internet. Puede agregar un proxy transparente o explícito. Los parámetros --proxy y --cacert son opcionales y no se le solicitará que los agregue. Si tiene un servidor proxy, deberá introducir los parámetros como se muestra.

A continuación se muestra un ejemplo de configuración de un servidor proxy explícito con un certificado firmado por una CA:

```
 ./BlueXP-Connector-Cloud-v3.9.40--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 un \ como se muestra anteriormente.
  - BlueXP no admite nombres de usuario ni contraseñas que incluyan el carácter @.
  - Si la contraseña incluye alguno de los siguientes caracteres especiales, debe escapar de ese carácter especial preponiéndolo con una barra diagonal inversa: & O !

    Por ejemplo:

    http://bxpproxyuser:netapp1\!@address:3128

--cacert especifica un certificado firmado por CA que se utilizará para el acceso HTTPS entre el conector y el servidor proxy. Este parámetro es necesario para servidores proxy HTTPS, servidores proxy de interceptación y servidores proxy transparentes.

A continuación se muestra un ejemplo de configuración de un servidor proxy transparente. Al configurar un proxy transparente, no es necesario definir el servidor proxy. Solo se agrega un certificado firmado por una CA al host del conector:

```
 ./BlueXP-Connector-Cloud-v3.9.40 --cacert
/tmp/cacert/certificate.cer
```

5. Si usó Podman, necesitará ajustar el puerto aardvark-dns.
   a. SSH a la máquina virtual del conector BlueXP.
   b. Abra el archivo podman */usr/share/containers/containers.conf* y modifique el puerto seleccionado para el servicio DNS de Aardvark. Por ejemplo, cámbielo a 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

   c. Reinicie la máquina virtual del conector.

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.

Antes de empezar

La persona que configura el conector BlueXP debe iniciar sesión en BlueXP mediante un inicio de sesión que no pertenezca a una cuenta u organización de BlueXP .

Si el inicio de sesión de BlueXP está asociado a otra cuenta u organización, deberá registrarse y obtener un nuevo inicio de sesión de BlueXP . De lo contrario, no verá la opción de habilitar el modo restringido en la pantalla de configuración.

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.

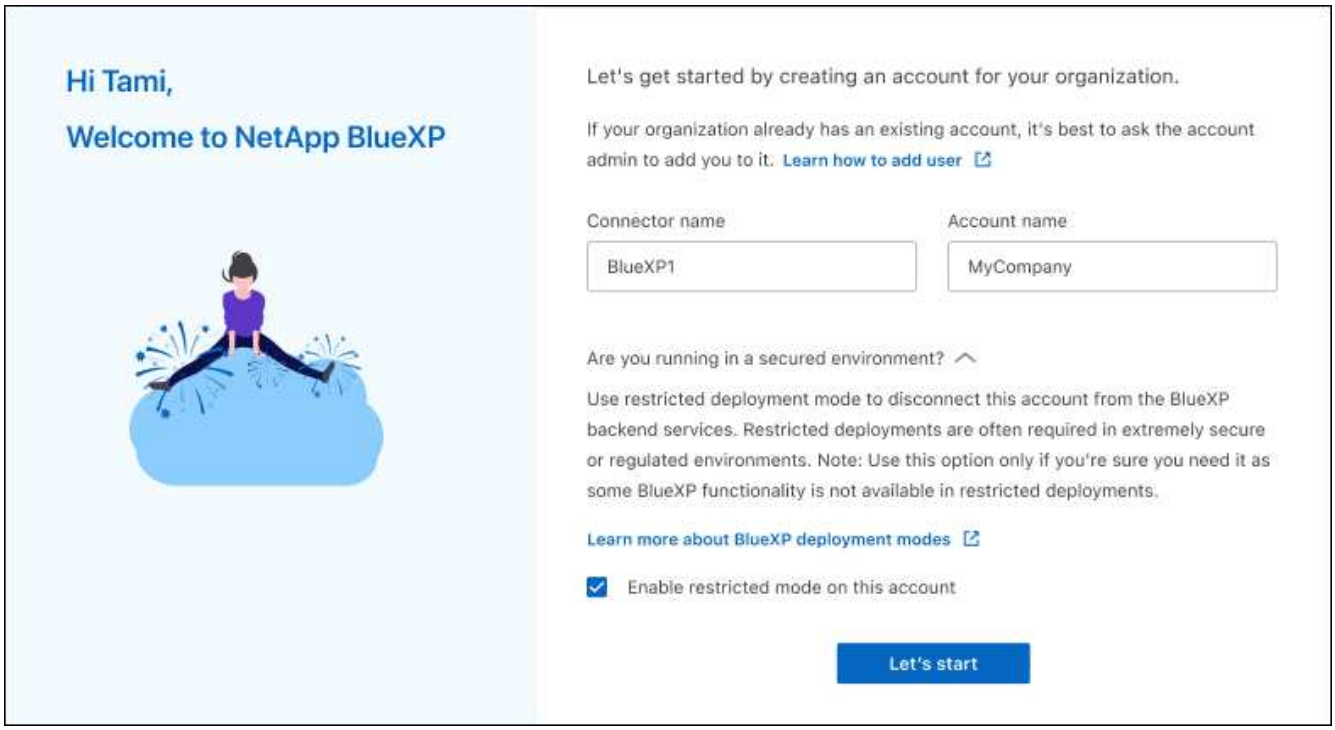
   b. Escriba un nombre para una nueva cuenta de BlueXP .

   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

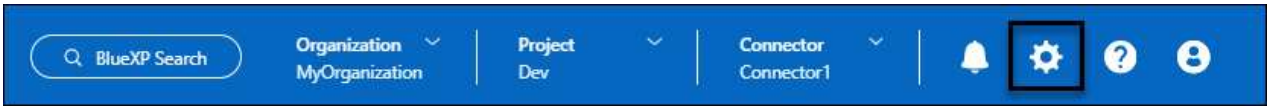
BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

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

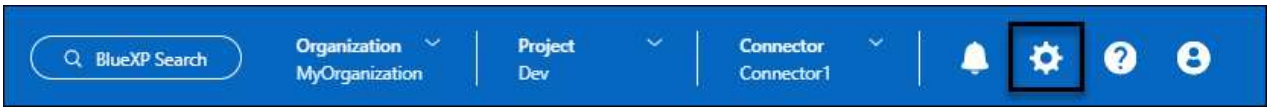
BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

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 NetApp Intelligent Services (modo restringido)

Suscríbete a NetApp Intelligent Services desde el marketplace de tu proveedor de nube para pagar los servicios de datos a una tarifa por hora (PAYGO) o mediante 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 de mercado permite cobrar por los siguientes servicios de datos con modo restringido:

- Backup y recuperación
- Cloud Volumes ONTAP
- Organización en niveles
- Protección contra ransomware
- Recuperación tras siniestros

La clasificación se habilita a través de su suscripción, pero no hay ningún cargo por utilizarla.

Antes de empezar

La suscripción a servicios de datos implica asociar una suscripción de mercado con las credenciales de la nube que están 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

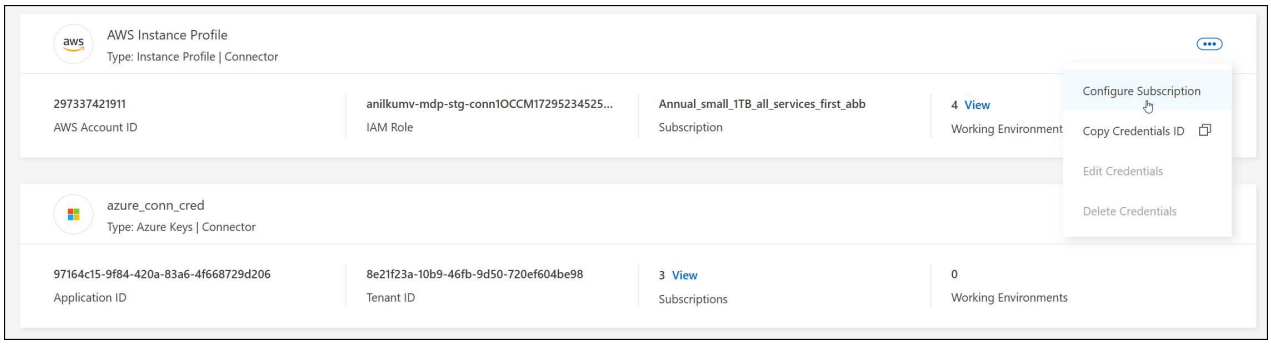
El siguiente vídeo muestra los pasos para suscribirse a NetApp Intelligent Services desde AWS Marketplace:

Suscríbase a NetApp Intelligent Services desde AWS Marketplace

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 **Configurar suscripción**.

   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 de la lista desplegable y seleccione **Configurar**.
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 organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
      - En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

        BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o 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 todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

◦ Seleccione **Guardar**.

Azure

Pasos

1. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Configurar suscripción**.

   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 de la lista desplegable y seleccione **Configurar**.
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**.

      Serás redirigido a BlueXP.

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

      - Seleccione las organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
      - En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

        BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o 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 todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

      - Seleccione **Guardar**.

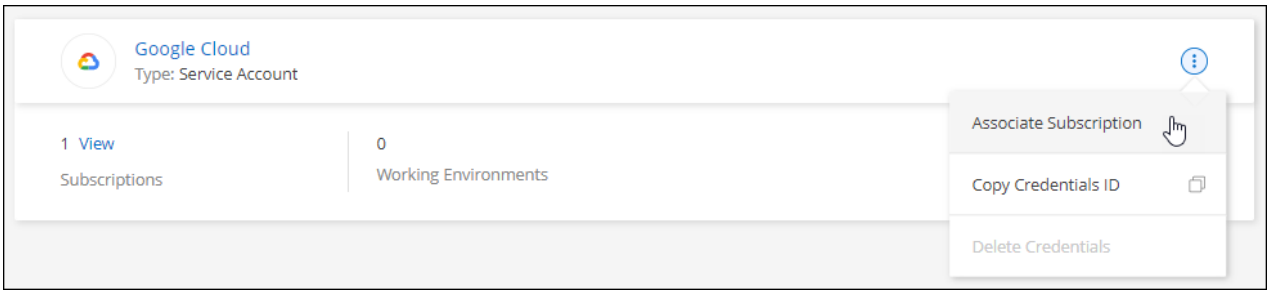
        En el siguiente vídeo se muestran los pasos para suscribirse desde Azure Marketplace:

   Suscríbase a NetApp Intelligent Services desde Azure Marketplace

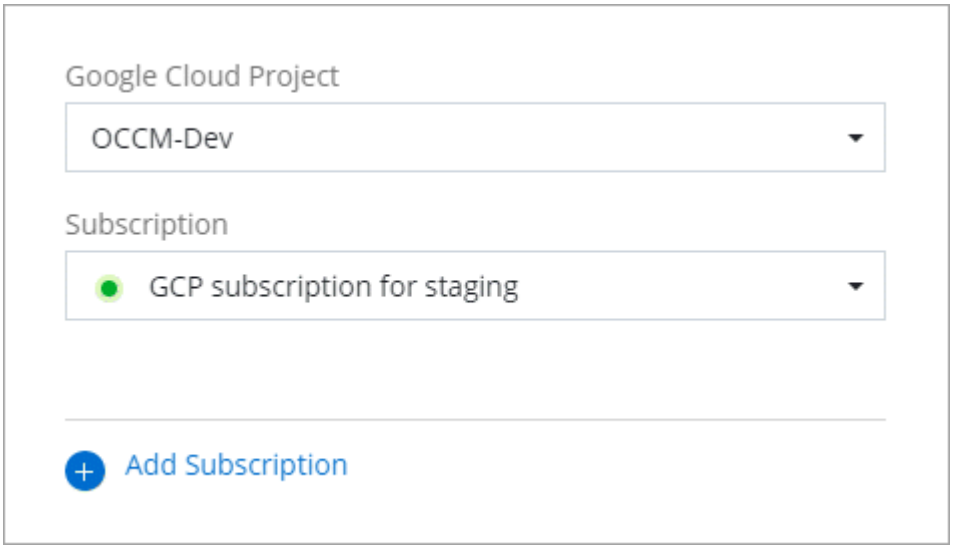
Google Cloud

Pasos

1. En la parte superior derecha de la consola, seleccione el ícono Configuración y seleccione **Credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Configurar suscripción**. +nueva captura de pantalla necesaria (TS)



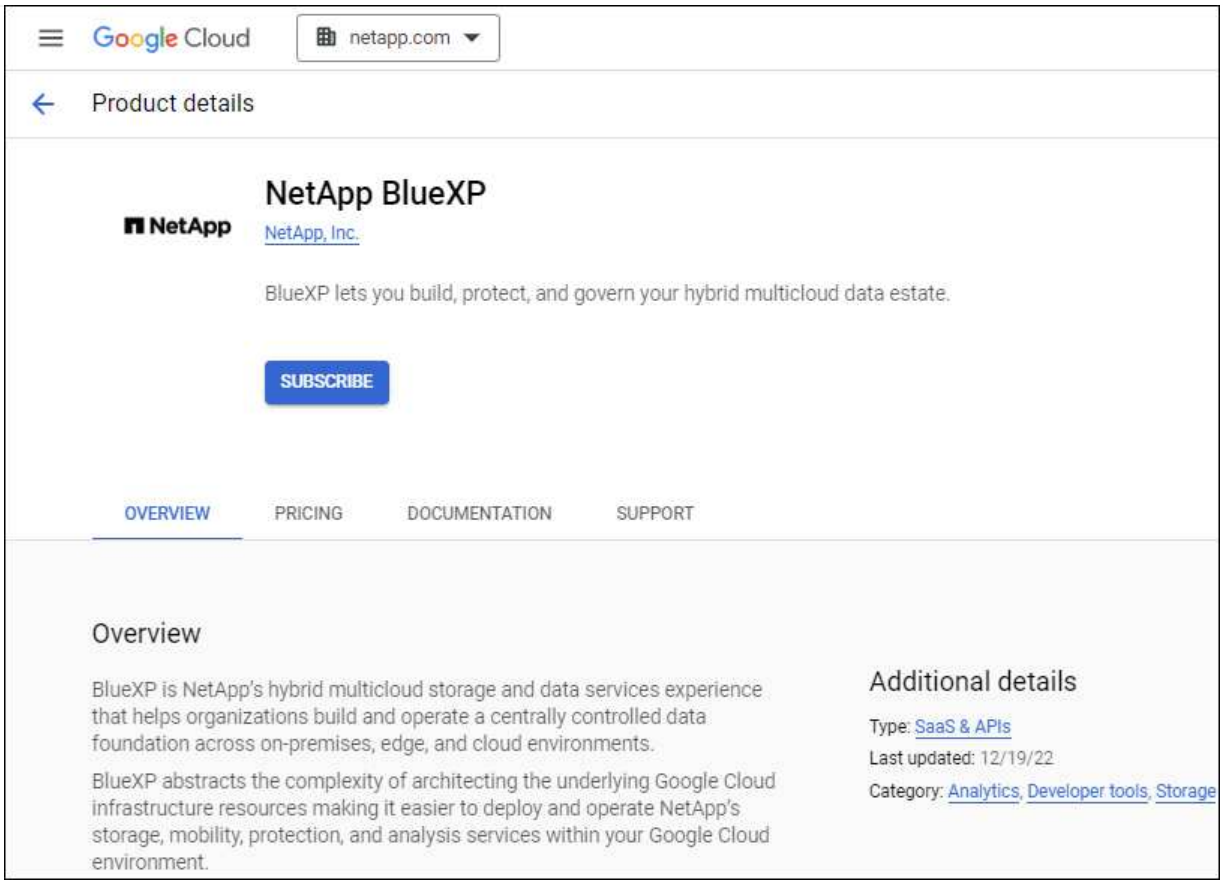
3. Para configurar una suscripción existente con las credenciales seleccionadas, seleccione un proyecto y una suscripción de Google Cloud en la lista desplegable y, a continuación, seleccione **Configurar**.



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. Después de ser redirigido a la "Página de Servicios inteligentes de NetApp en Google Cloud Marketplace" , asegúrese de que el proyecto correcto esté seleccionado en el menú de navegación superior.

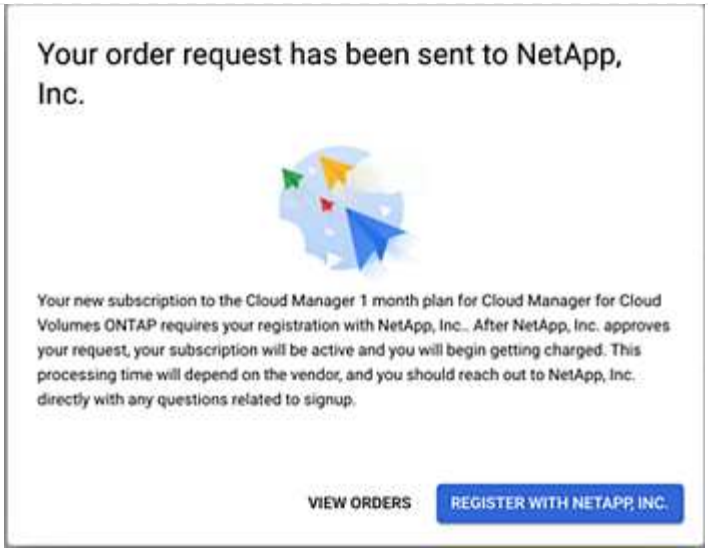


b. Seleccione **Suscribirse**.
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.
d. Seleccione **Suscribirse**.

   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 con tu organización o 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 organizaciones o cuentas de BlueXP con las que desea asociar esta suscripción.
- En el campo **Reemplazar suscripción existente**, elige si deseas reemplazar automáticamente la suscripción existente para una organización o cuenta con esta nueva suscripción.

  BlueXP reemplaza la suscripción existente para todas las credenciales de la organización o 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.

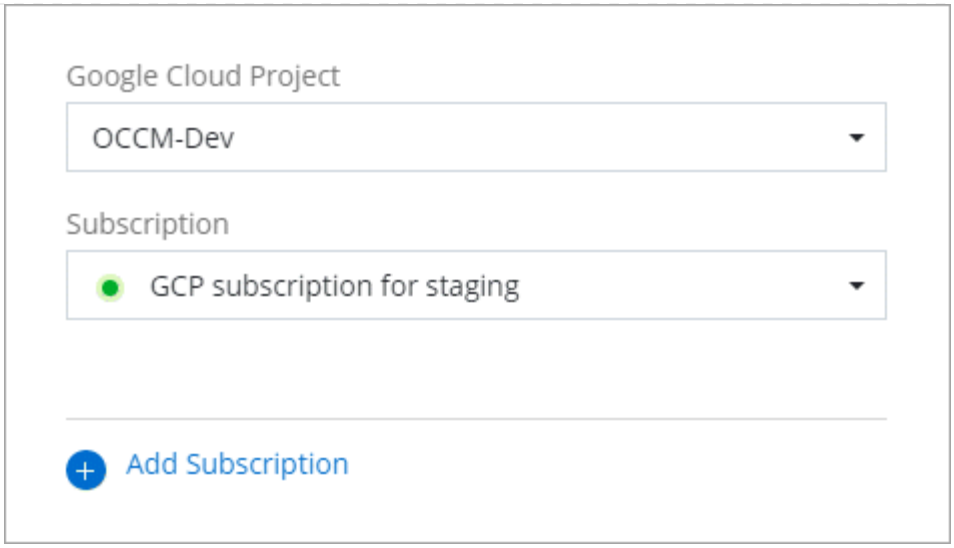
Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- 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.



Información relacionada

- "Gestione las licencias basadas en la capacidad de su propia licencia para Cloud Volumes ONTAP"
- "Administrar licencias BYOL para servicios de datos"
- "Administrar credenciales y suscripciones de AWS"
- "Administrar credenciales y suscripciones de Azure"
- "Administrar credenciales y suscripciones de Google Cloud"

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 Azure NetApp Files"
- "Documentos de backup y recuperación"
- "Documentos de clasificación"
- "Documentos de Cloud Volumes ONTAP"
- "Documentos de la cartera digital"
- "Documentos del clúster ONTAP en las instalaciones"
- "Documentos de replicación"

Información relacionada

"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 comenzar, debe tener un entendimiento de "Conectores" y. "modos de despliegue"

1 "Prepárese para la puesta en marcha"

1. Prepare un host Linux dedicado que cumpla con los requisitos de CPU, RAM, espacio en disco, herramienta de orquestación de contenedores y 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.

Para utilizar BlueXP en el "Cloud secreto de AWS" o el "Cloud secreto principal de AWS" , siga las instrucciones específicas para 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 comenzar, debes comprender el modo privado.

Por ejemplo, debe utilizar la interfaz basada en navegador que está disponible localmente desde el Conector que instale. No puede acceder a BlueXP desde la consola basada en Web que se proporciona a través de la capa SaaS.

Además, no todas las funciones y servicios están disponibles.

"Aprenda cómo funciona el modo privado".

Paso 2: Revise las opciones de instalación

En el modo privado, puede instalar el conector en las instalaciones o en la nube instalando manualmente el conector en su propio host Linux.

Dónde instalas Connector determina los servicios y características de BlueXP que están disponibles cuando se utiliza el modo privado. Por ejemplo, el conector debe estar instalado en la nube si desea desplegar y administrar Cloud Volumes ONTAP. "Obtenga más información sobre el modo privado".

Paso 3: Revise los requisitos del host

El host debe cumplir con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de puerto, etc. para ejecutar el software del conector.

Host dedicado

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

Host puede ser de cualquier arquitectura que cumpla con los siguientes requisitos de tamaño:

- CPU: 8 núcleos o 8 vCPU
- RAM: 32 GB

Requisitos del sistema operativo y del contenedor

BlueXP admite el conector con los siguientes sistemas operativos cuando se utiliza BlueXP en modo privado. Antes de instalar el conector, se necesita una herramienta de orquestación de contenedores.

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10	3.9.42 o posterior con BlueXP en modo privado	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	22,04 LTS	3.9.29 o posterior	Docker Engine 23.0.6 a 26.0.0 26.0.0 es compatible con *NEW* Connector 3.9.44 o instalaciones posteriores	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en 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.

Hipervisor

Se requiere un hipervisor nativo o alojado que esté certificado para ejecutar un sistema operativo compatible.

CPU

8 núcleos o 8 vCPU

RAM

32GB

Tipo de instancia de AWS EC2

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos t3.2xlarge.

Tamaño de la máquina virtual de Azure

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos Standard_D8s_v3.

Tipo de máquina de Google Cloud

Tipo de instancia que cumple los requisitos anteriores de CPU y RAM. Recomendamos n2-standard-8.

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

BlueXP utiliza `/opt` para instalar el `/opt/application/netapp` directorio y su contenido.

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

BlueXP requiere este espacio en `/var` Porque Docker o Podman están diseñados para crear los contenedores dentro de este directorio. Específicamente, crearán contenedores en el `/var/lib/containers/storage` directorio. Los montajes externos o los enlaces simbólicos no funcionan en este espacio.

Paso 4: Instale Podman o Docker Engine

Debe preparar el host para el conector instalando Podman o Docker Engine.

Dependiendo del sistema operativo, se requiere Podman o Docker Engine antes de instalar el conector.

- Se requiere Podman para Red Hat Enterprise Linux 8 y 9.

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 6. Pasos

Podman

Siga estos pasos para instalar Podman y configurarlo para cumplir con los siguientes requisitos:

- Habilitar e iniciar el servicio podman.socket
- Instale python3
- Instalar el paquete podman-compose versión 1.0.6
- Agregue podman-compose a la variable de entorno PATH

Al usar Podman, ajuste el puerto del servicio aardvark-dns (predeterminado: 53) después de instalar el Conector para evitar conflictos con el puerto DNS del host. Siga las instrucciones para configurar el puerto.

Pasos

1. Elimine el paquete podman-docker si está instalado en el host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Instale Podman.

   Podman está disponible en repositorios oficiales de Red Hat Enterprise Linux.

   Para Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

   Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

   Donde <version> es la versión compatible de Podman que está instalando. Ver las versiones de Podman que admite BlueXP .

3. Active e inicie el servicio podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Instale python3.

```
sudo dnf install python3
```

5. Instale el paquete de repositorio de EPEL si aún no está disponible en su sistema.

   Este paso es necesario porque podman-compose está disponible en el repositorio Extra Packages for Enterprise Linux (EPEL).

   Para Red Hat Enterprise Linux 9:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
   ```

   Para Red Hat Enterprise Linux 8:

   ```
   sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
   ```

6. Instale el paquete podman-compose 1,0.6.

   ```
   sudo dnf install podman-compose-1.0.6
   ```

   Con el `dnf install` El comando cumple con los requisitos para agregar podman-compose a la variable de entorno PATH. El comando installation agrega podman-compose a /usr/bin, que ya está incluido en el `secure_path` opción en el host.

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

   Asegúrese de seguir los pasos para instalar una versión específica de Docker Engine. Al instalar la versión más reciente se instalará una versión de Docker no compatible con BlueXP.

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 5: Preparar el networking

Configure la red del Conector para administrar recursos en su nube pública. Además de tener una red virtual y una subred para el Conector, asegúrese de que se cumplan los siguientes requisitos. Conexiones a redes de

destino: El Conector debe tener una conexión de red a la ubicación donde planea administrar 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.

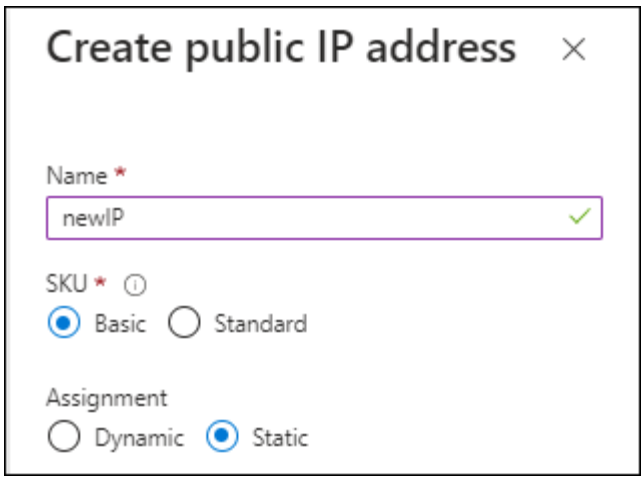
Extremos para operaciones del día a día

Si está planeando crear sistemas Cloud Volumes ONTAP, el conector necesita conectividad con los extremos de los recursos disponibles públicamente de su proveedor de cloud.

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.
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

NetApp admite configuraciones de proxy explícitas y transparentes. Si usa un proxy transparente, solo necesita proporcionar el certificado del servidor proxy. Si usa un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Credenciales
- Certificado HTTPS

  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 6: Preparar permisos en la nube

Si el conector está instalado en la nube y planea crear sistemas Cloud Volumes ONTAP, BlueXP requiere permisos del proveedor de la nube. 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.

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. Proporcione 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. Asigne esta función a la máquina virtual del conector.

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.

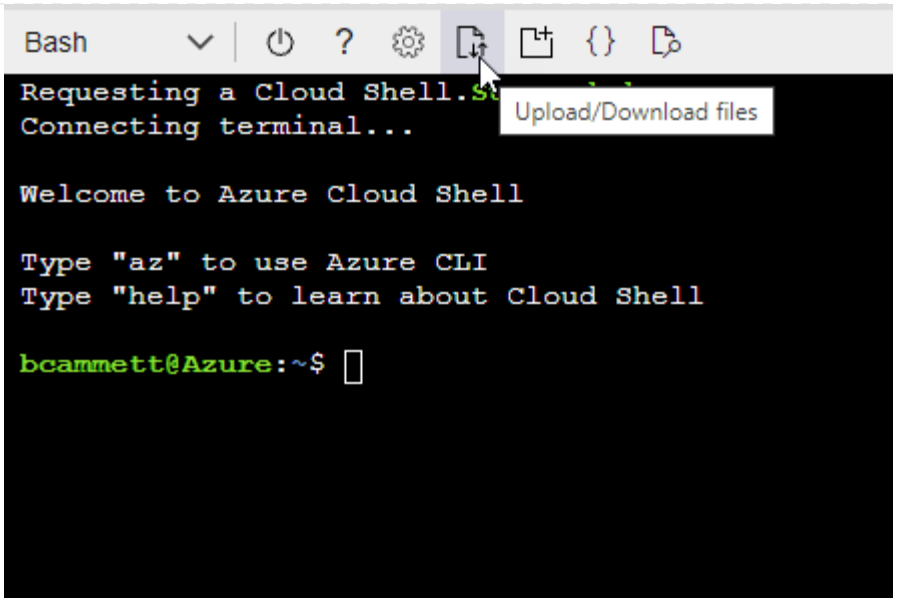
   ejemplo

   ```
   "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

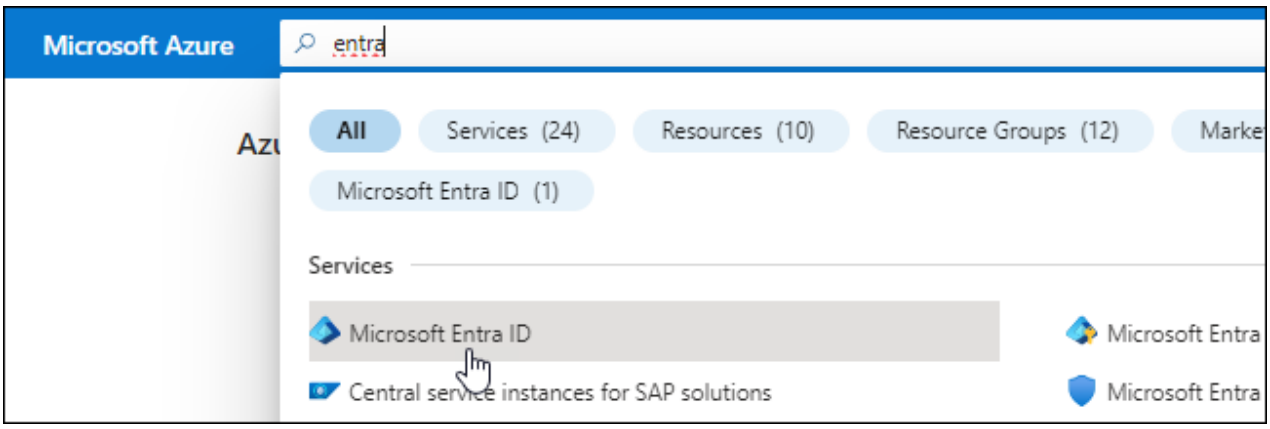
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita. Necesitará proporcionar estas credenciales a BlueXP después de instalar el conector y configurar BlueXP.

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.

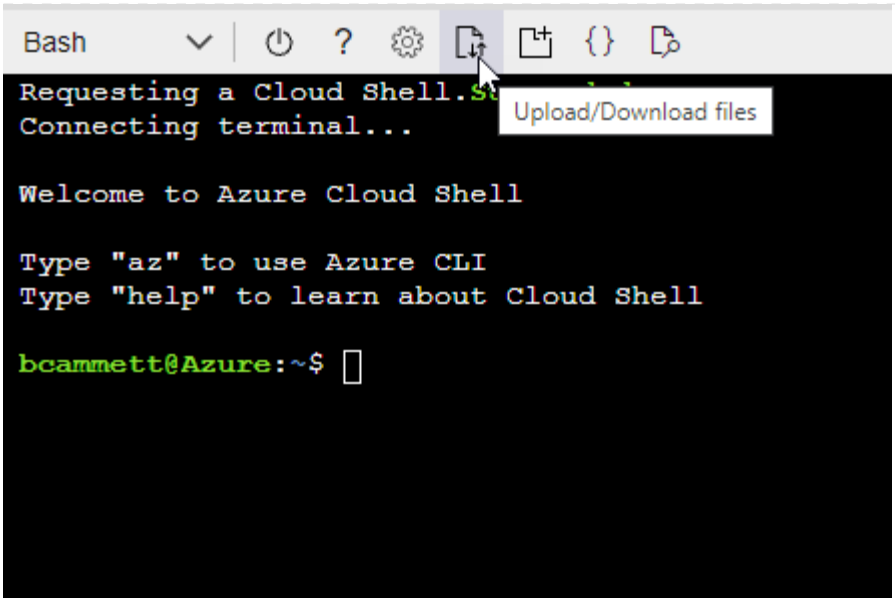
      ejemplo

      ```
      "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:

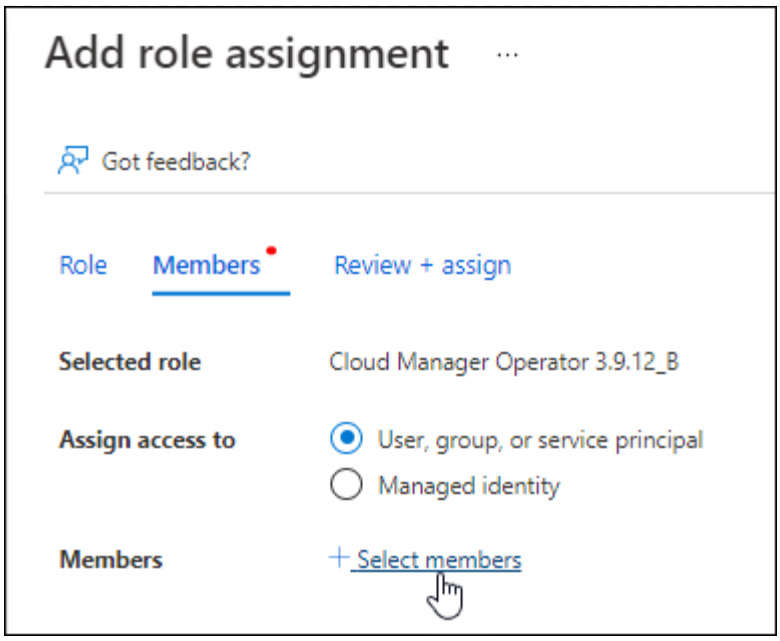
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

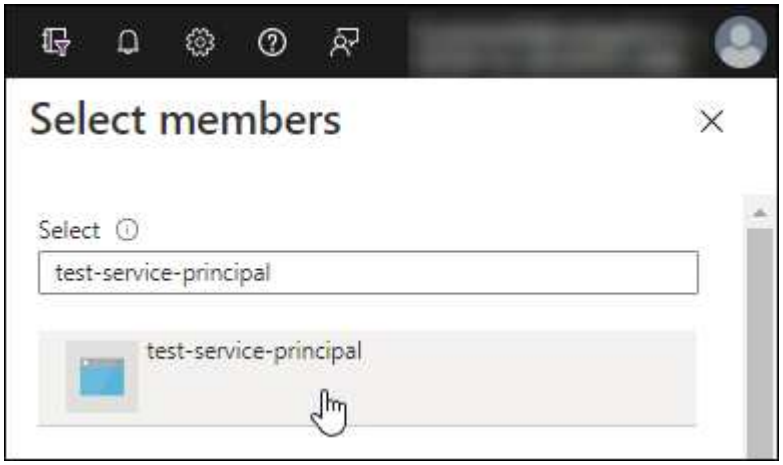
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**,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

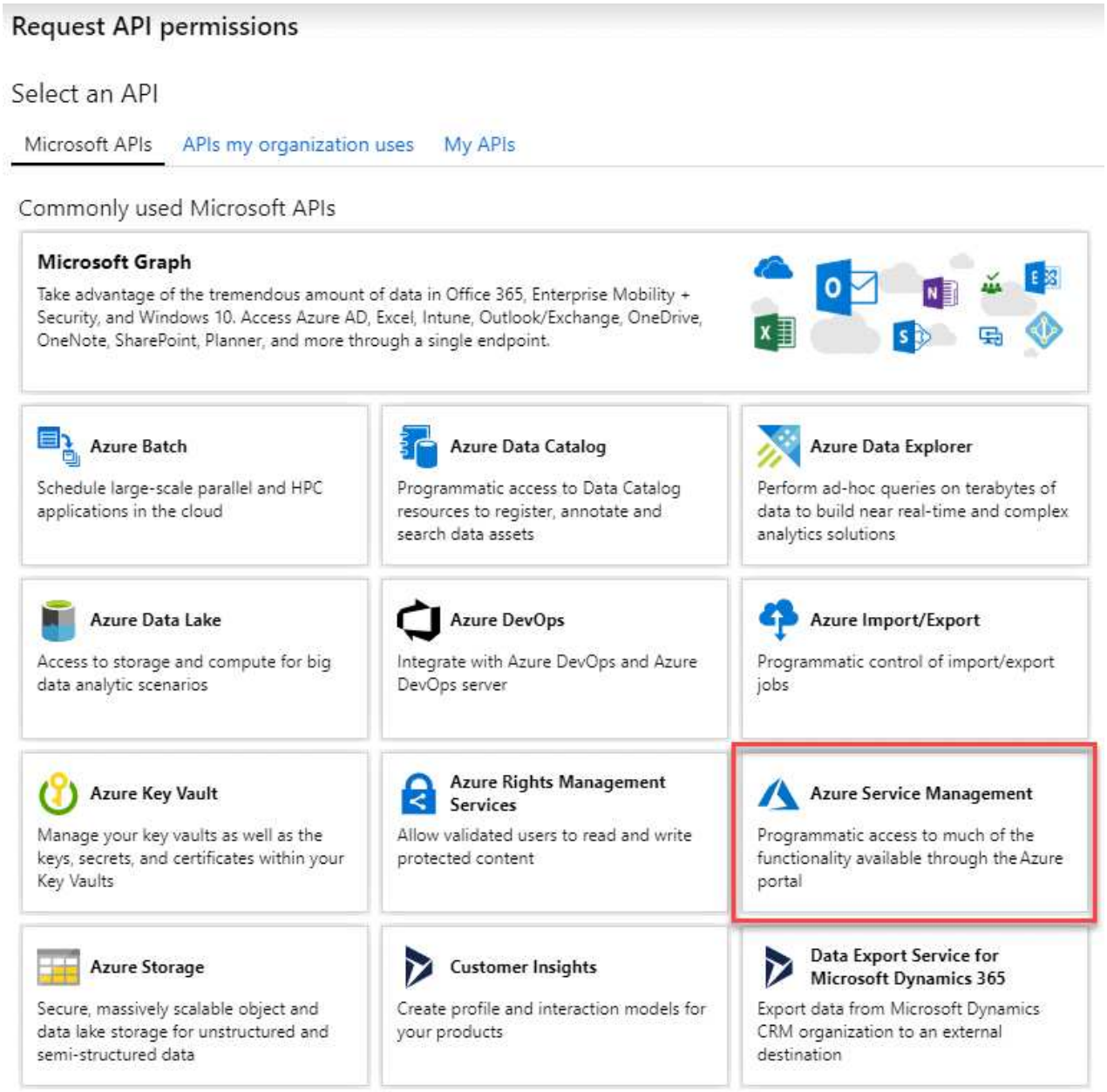
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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.

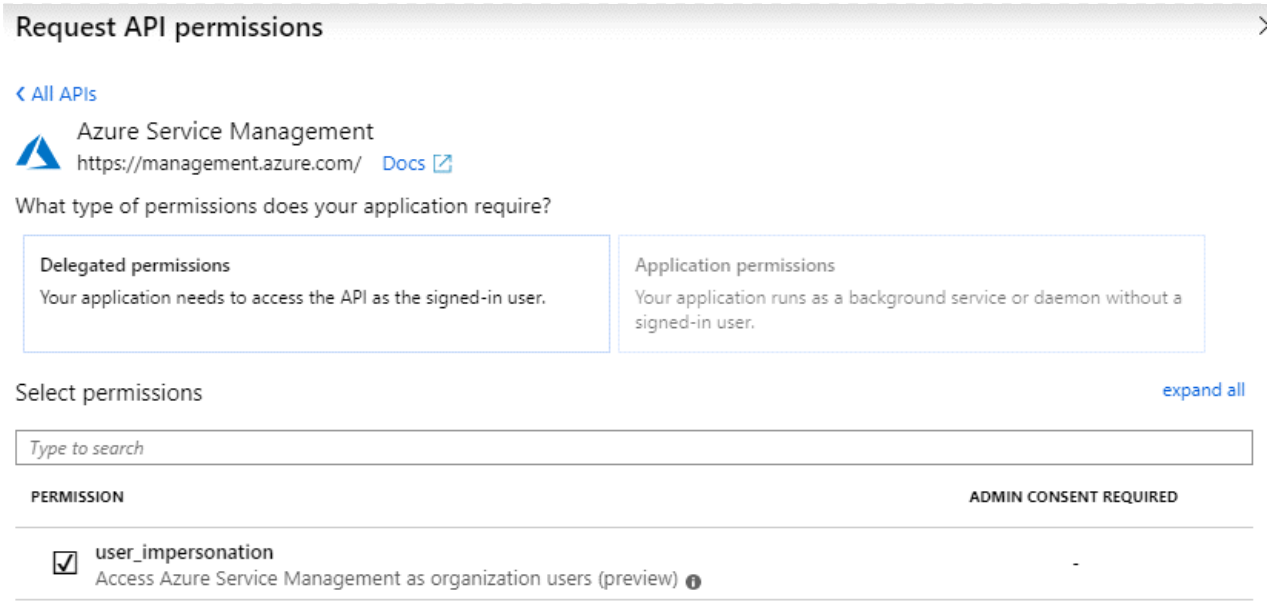
Añada permisos de API de administración de servicios de Windows Azure

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**.

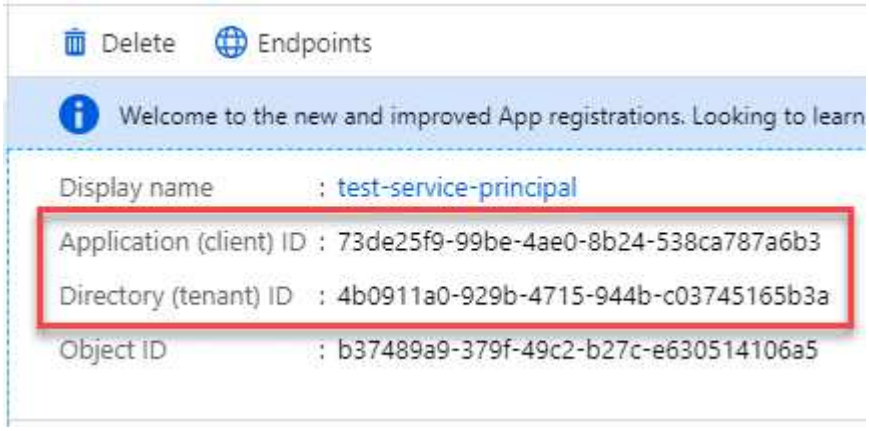


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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. Ingrese esta información en BlueXP cuando agregue 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 7: Habilita las API de Google Cloud

Debe habilitar varias API para implementar 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

Implemente el conector en modo privado para que pueda utilizar BlueXP sin conectividad saliente a la capa de software como servicio (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

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.
- Dependiendo del sistema operativo, se requiere Podman o Docker Engine antes de instalar el conector.

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.

Resultado

El software del conector está instalado. Ya puede configurar BlueXP.

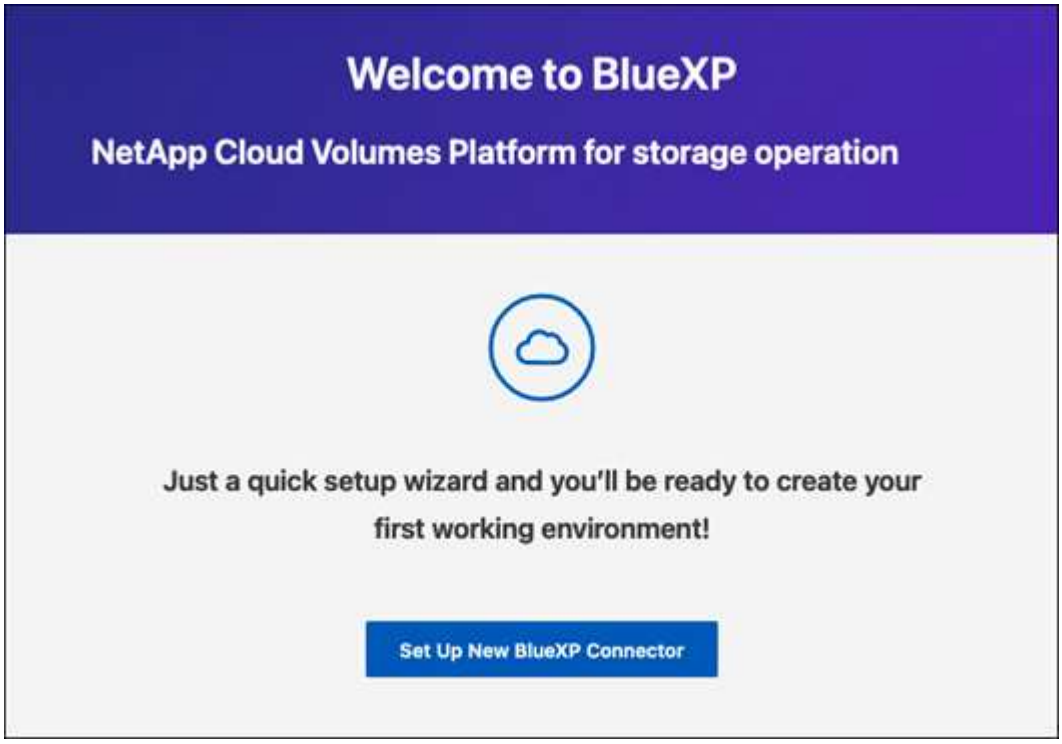
Paso 2: Configura BlueXP

Cuando acceda a la consola BlueXP por primera vez, se le solicitará que configure BlueXP.

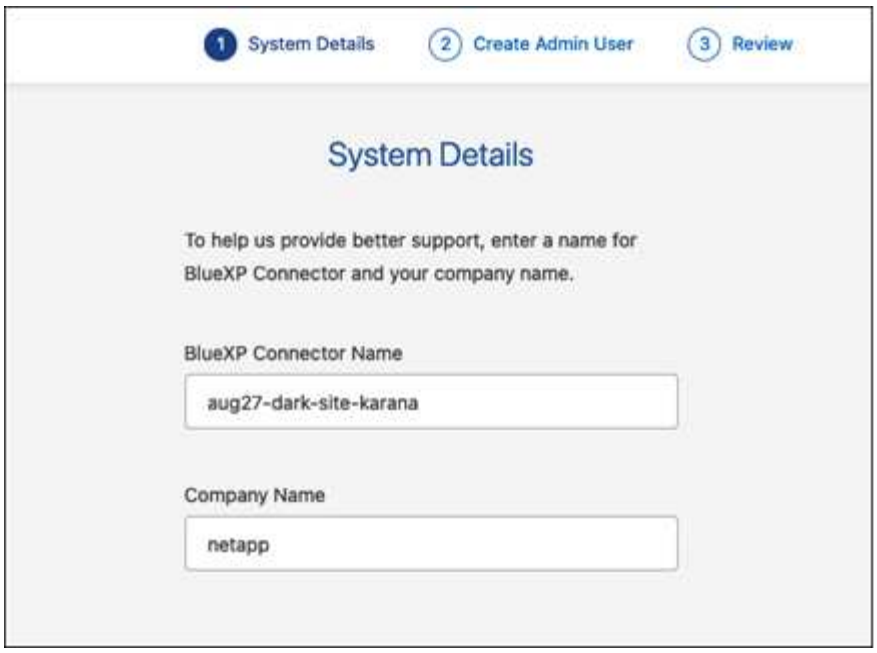
Pasos

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

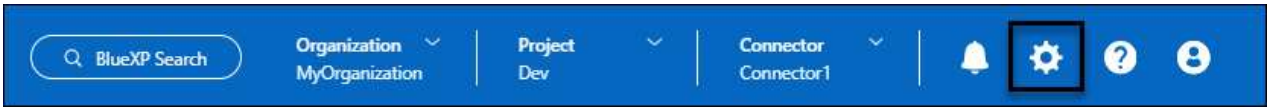
BlueXP dispone ahora de los permisos que necesita para realizar acciones en AWS en su nombre.

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

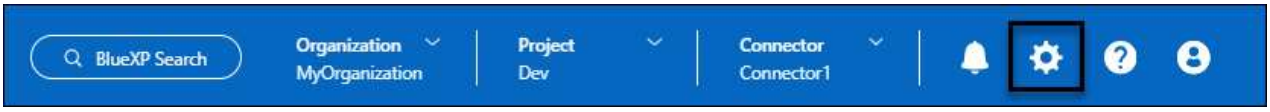
BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

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:

- "Detectar clústeres de ONTAP en las instalaciones"
- "Gestionar actualizaciones de software"
- "Escanee los datos de volumen de ONTAP locales mediante la clasificación de BlueXP"
- "Supervise el uso de las licencias con la cartera digital"
- "Consulte la información de estado del almacenamiento con el asesor digital"