



Comience con el modo privado

BlueXP setup and administration

NetApp
April 08, 2025

Tabla de contenidos

- Comience con el modo privado 1
 - Flujo de trabajo inicial (modo privado) 1
 - Preparación para la implementación en modo privado 1
 - Paso 1: Entender cómo funciona el modo privado 1
 - Paso 2: Revise las opciones de instalación 2
 - Paso 3: Revise los requisitos del host 2
 - Paso 4: Instale Podman o Docker Engine 3
 - Paso 5: Preparar el networking 5
 - Paso 6: Preparar permisos en la nube 7
 - Paso 7: Habilita las API de Google Cloud 18
- Despliegue el conector en modo privado 18
 - Paso 1: Instale el conector 18
 - Paso 2: Configura BlueXP 19
 - Paso 3: Proporcionar permisos a BlueXP 20
- Cuentas BlueXP 23
 - Obtenga más información sobre las cuentas de BlueXP 23
 - Administre su cuenta de BlueXP 24
- Qué puede hacer después (modo privado) 29

Comience con el modo privado

Flujo de trabajo inicial (modo privado)

Empieza a usar BlueXP en modo privado preparando tu entorno y poniendo en marcha Connector.

El modo privado se suele utilizar con entornos locales que no tienen conexión a Internet y con regiones de nube seguras, lo que incluye ["Cloud secreto de AWS"](#), ["Cloud secreto principal de AWS"](#), y ["Azure IL6"](#)

Antes de empezar, debería comprender ["Cuentas BlueXP"](#), ["Conectores"](#), y ["modos de despliegue"](#).

1

"Prepárese para la puesta en marcha"

1. Prepare un host 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.



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

Paso 1: Entender cómo funciona el modo privado

Antes de empezar, debe comprender cómo funciona BlueXP en modo privado.

Por ejemplo, debe entender que necesita utilizar la interfaz basada en explorador que está disponible localmente desde el conector BlueXP que necesita instalar. No puede acceder a BlueXP desde la consola basada en Web que se proporciona a través de la capa SaaS.

Además, no todos los servicios de BlueXP están disponibles.

["Aprenda cómo funciona el modo privado"](#).

Paso 2: Revise las opciones de instalación

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

Host dedicado

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

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	Versión de OS compatibles	Versión 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 <i>NEW</i> 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 1. Pasos

Podman

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

- El servicio podman.socket debe estar activado e iniciado
- se debe instalar python3
- Se debe instalar el paquete de composición podman versión 1.0.6
- Se debe agregar la composición podman a la variable de entorno PATH

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.

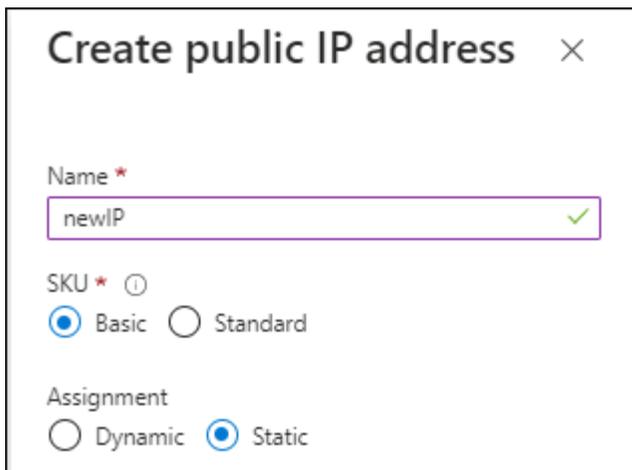
Extremos para operaciones del día a día

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): <ul style="list-style-type: none">• 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.



Create public IP address ✕

Name *
newIP ✓

SKU * ⓘ
 Basic Standard

Assignment
 Dynamic Static

Si en su lugar utiliza una dirección IP de SKU estándar, BlueXP utiliza la dirección *private* IP del conector, en lugar de la dirección IP pública. Si el equipo que está utilizando para acceder a la consola BlueXP no tiene acceso a esa dirección IP privada, las acciones de la consola BlueXP fallarán.

["Documentación para Azure: SKU de IP pública"](#)

Servidor proxy

Si su empresa requiere la implementación de un servidor proxy para todo el tráfico de Internet saliente, obtenga la siguiente información sobre su proxy HTTP o HTTPS. Deberá proporcionar esta información durante la instalación. Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.

- 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 Connector está instalado en la nube y tiene pensado crear sistemas Cloud Volumes ONTAP, BlueXP requiere permisos de su proveedor de 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. Seleccione **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. Seleccione **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. Seleccione **Políticas > Crear política**.
 - b. Seleccione **JSON** y copie y pegue el contenido del ["Política de IAM para el conector"](#).
 - c. Finalice los pasos restantes para crear la directiva.

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

Para las regiones estándar, los permisos se distribuyen en dos directivas. Son necesarias dos políticas debido a un límite máximo de tamaño de carácter para las políticas gestionadas en AWS. ["Obtenga más información sobre las políticas de IAM para el conector"](#).

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

Resultado

La cuenta ahora tiene los permisos necesarios.

Rol de Azure

Cree un rol personalizado de Azure con los permisos necesarios. Asignará este rol al conector VM.

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

Pasos

1. Habilite una identidad administrada asignada por el sistema en la máquina virtual donde tenga pensado instalar el conector de modo que pueda proporcionar los permisos de Azure necesarios a través de una función personalizada.

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

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

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

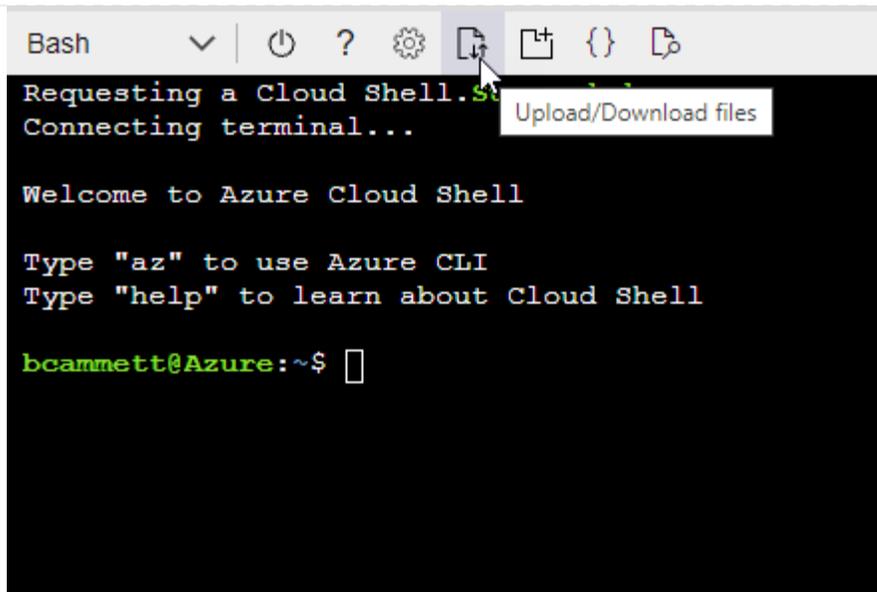
ejemplo

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

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

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

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



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

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

Resultado

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

Servicio principal de Azure

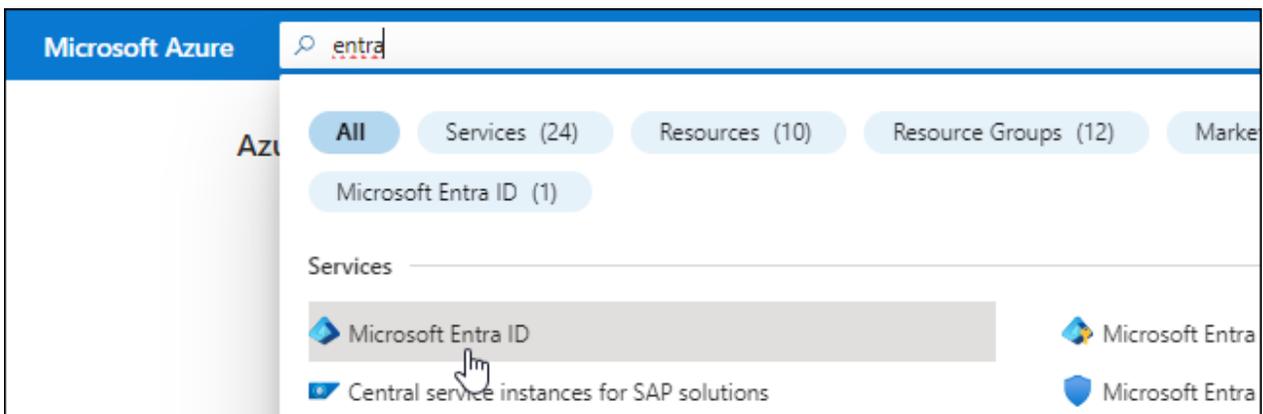
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita. Necesitará proporcionar estas credenciales a BlueXP después de instalar el conector y configurar BlueXP.

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

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

Para obtener más información, consulte ["Documentación de Microsoft Azure: Permisos necesarios"](#)

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



3. En el menú, seleccione **App registrs**.
4. Seleccione **Nuevo registro**.
5. Especificar detalles acerca de la aplicación:
 - **Nombre:** Introduzca un nombre para la aplicación.
 - **Tipo de cuenta:** Seleccione un tipo de cuenta (cualquiera funcionará con BlueXP).
 - **Redirigir URI:** Puede dejar este campo en blanco.
6. Seleccione **Registrar**.

Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

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

- a. Copie el contenido de "[Permisos de función personalizada para el conector](#)" Y guárdelos en un archivo JSON.
- b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

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

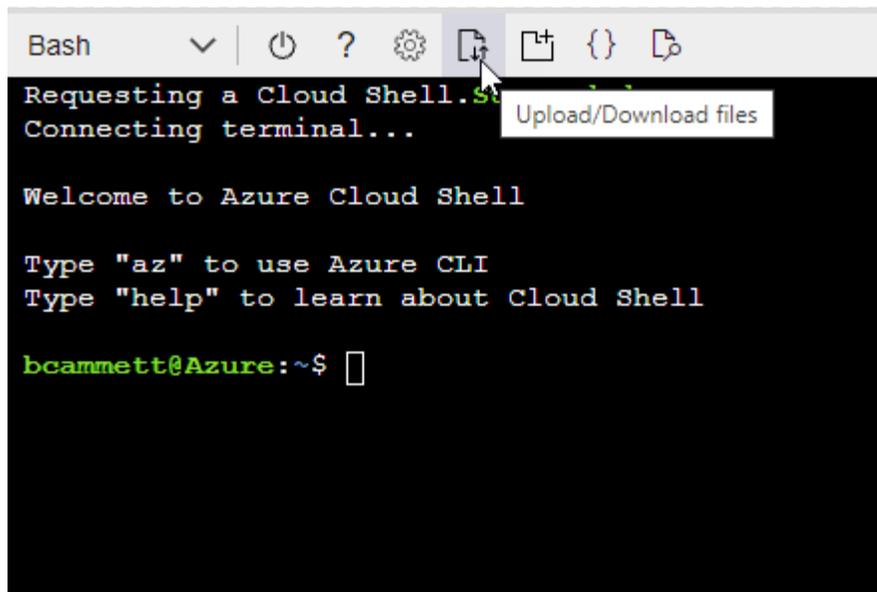
ejemplo

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

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

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

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



```
Bash
Requesting a Cloud Shell.
Connecting terminal...
Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

bcammett@Azure:~$
```

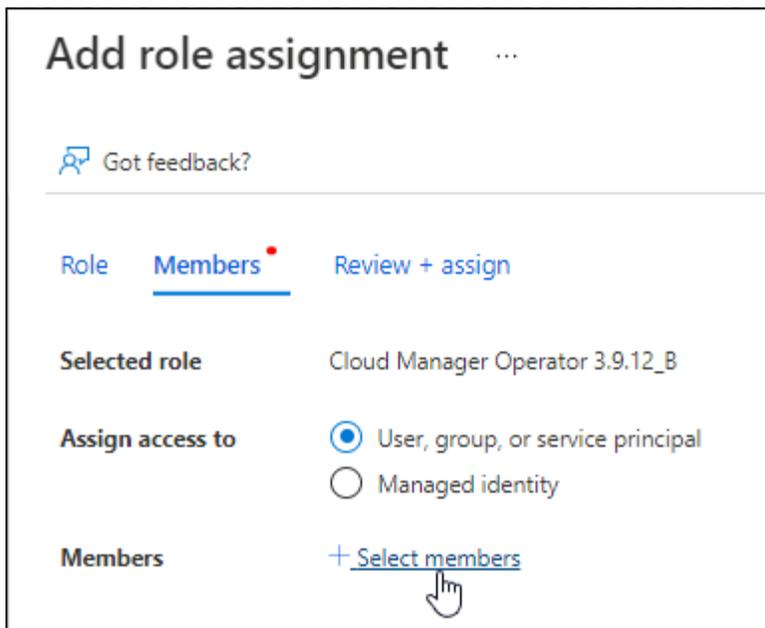
- Use la interfaz de línea de comandos de Azure para crear el rol personalizado:

```
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.

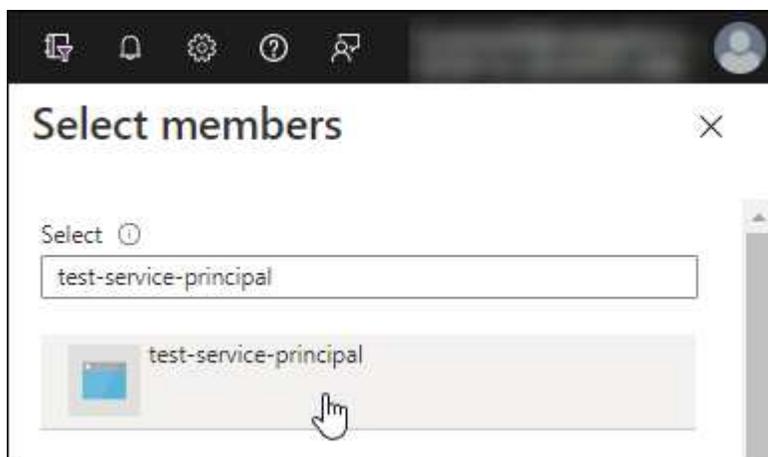
2. Asigne la aplicación al rol:

- 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**.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



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

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user_impersonation

Access Azure Service Management as organization users (preview)

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)**.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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 conector` comando.

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

```
gcloud iam roles create conector --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 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.

1 System Details 2 Create Admin User 3 Review

System Details

To help us provide better support, enter a name for BlueXP Connector and your company name.

BlueXP Connector Name

Company Name

- **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](#)

2. Seleccione **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. Seleccione **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.

Cuentas BlueXP

Obtenga más información sobre las cuentas de BlueXP

Cuando utilice BlueXP en modo privado, utilizará una cuenta *BlueXP* para administrar usuarios y organizar recursos en un *workspace* aislado.

Si usas BlueXP en modo estándar o restringido, no tendrás una cuenta de BlueXP. En su lugar, dispondrá de una organización *BlueXP* que gestionará mediante la administración de identidades y accesos (IAM) de BlueXP.

- ["Obtenga más información sobre BlueXP IAM"](#)
- ["Obtenga más información sobre los modos de implementación de BlueXP"](#)

Descripción general

Cuando accede por primera vez a BlueXP, ya se crea una cuenta para usted con un espacio de trabajo llamado *Workspace-1*.

A continuación, puede agregar miembros (usuarios) a esta cuenta e implementar conectores:

The screenshot shows the 'Manage Account: KeystoneTes...' interface. At the top, there are navigation tabs: 'Overview' (selected), 'Members', 'Workspaces', and 'BlueXP Connector'. Below the navigation, a summary bar displays three metrics: 30 Members, 1 Workspaces, and 3 Connectors. The main content area is divided into two rows. The first row shows 'KeystoneTest01' as the Account Name, with an edit icon and a toggle for 'Allow Private Preview'. The second row shows 'account-Pq7bhQxz' as the Account ID, with a copy icon and a toggle for 'Allow Third Party Services'.

["Aprenda a administrar su cuenta de BlueXP"](#).

Miembros

Los miembros son usuarios de BlueXP que usted asocia con su cuenta de BlueXP. La asociación de un usuario a una cuenta y su espacio de trabajo en esa cuenta permite a esos usuarios crear y gestionar entornos de trabajo en BlueXP .

Espacio de trabajo

En BlueXP, un área de trabajo aísla cualquier número de *entornos de trabajo* de otros usuarios de la cuenta. Los usuarios (miembros) de BlueXP no pueden acceder a los entornos de trabajo de un espacio de trabajo a menos que estén asociados a ese espacio de trabajo.

Un entorno de trabajo representa sistemas de almacenamiento como su clúster ONTAP en las instalaciones.

El modo privado de BlueXP sólo admite un espacio de trabajo.

Conectores

Un conector ejecuta las acciones que BlueXP necesita realizar para gestionar su infraestructura de datos. El conector se ejecuta en una instancia de máquina virtual que se implementa en su proveedor de cloud o en un host en las instalaciones que haya configurado.

Puede utilizar un conector con más de un servicio BlueXP. Por ejemplo, si utiliza un conector para gestionar las copias de seguridad y la recuperación, puede utilizar ese mismo conector con otro servicio como la organización en niveles de BlueXP .

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

Administre su cuenta de BlueXP

Cuando usas BlueXP en modo privado, usarás una cuenta *BlueXP* para administrar

usuarios y organizar recursos. Cuando creas tu cuenta, solo incluye un solo usuario y un espacio de trabajo. Puede administrar la cuenta para que se adapte a sus necesidades agregando usuarios y creando cuentas de servicio con fines de automatización.

Si usas BlueXP en modo estándar o restringido, no tendrás una cuenta de BlueXP. En su lugar, dispondrá de una organización *BlueXP* que gestionará mediante la administración de identidades y accesos (IAM) de BlueXP.

- ["Obtenga más información sobre BlueXP IAM"](#)
- ["Obtenga más información sobre los modos de implementación de BlueXP"](#)

Gestione su cuenta con la API de tenancy

Si desea administrar la configuración de su cuenta enviando solicitudes de API, deberá utilizar la API *Tenancy*. Esta API es diferente a la API de BlueXP. Tenga en cuenta que no puede crear nuevas cuentas o espacios de trabajo en modo privado, incluso con la API.

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

Cambie el nombre del espacio de trabajo

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

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.
2. Seleccione **espacios de trabajo**.
3. Seleccione **Cambiar nombre** para cambiar el nombre del espacio de trabajo.

Cambie el nombre de su cuenta

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

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.
2. En la ficha **Descripción general**, seleccione el icono de edición junto al nombre de la cuenta.
3. Escriba un nuevo nombre de cuenta y seleccione **Guardar**.

Crear y administrar usuarios

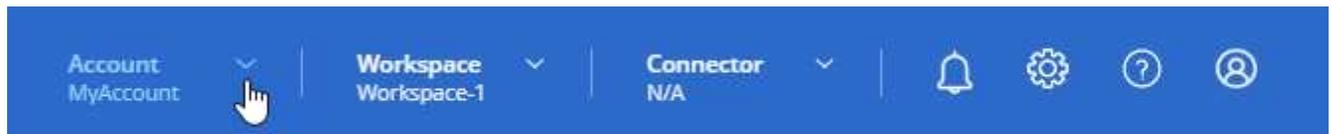
Los usuarios de su cuenta pueden acceder y gestionar los recursos del espacio de trabajo.

Añadir usuarios

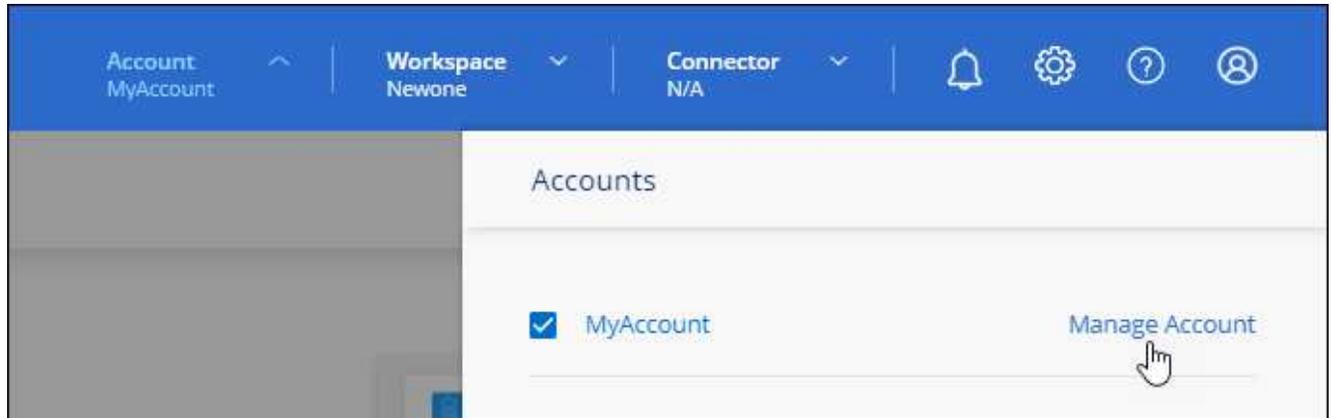
Asocie usuarios a su cuenta de BlueXP para que esos usuarios puedan crear y administrar entornos de trabajo en BlueXP.

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta**.



2. Seleccione **Administrar cuenta** junto a la cuenta seleccionada actualmente.



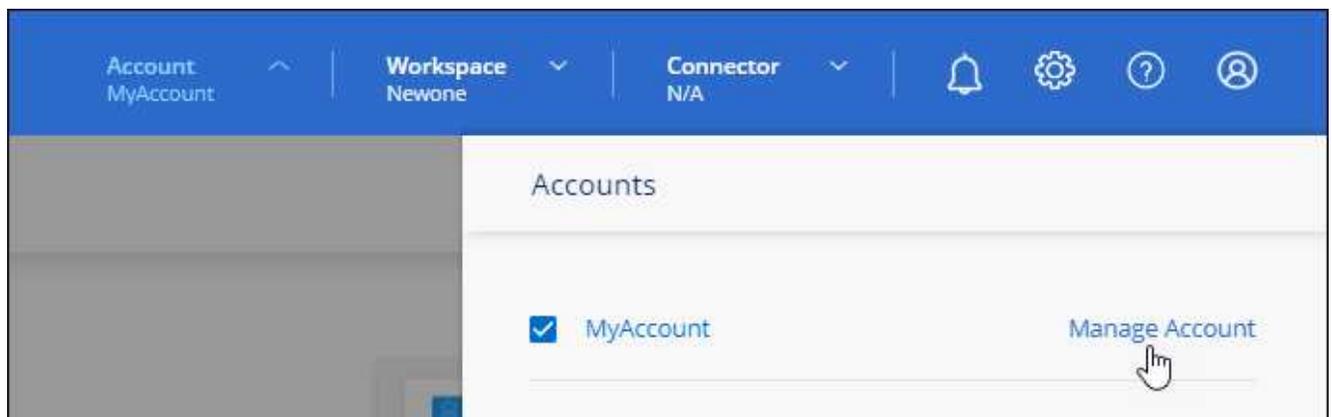
3. En la ficha Miembros, seleccione **Usuario asociado**.
4. Introduzca la dirección de correo electrónico del usuario.
5. Seleccione **asociado**. El usuario debe recibir un correo electrónico de NetApp BlueXP titulado "Asociación de cuentas". El correo electrónico incluye la información necesaria para acceder a BlueXP .

Elimine usuarios de su cuenta

Al desasociar un usuario, ya no pueden acceder a los recursos de una cuenta de BlueXP.

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta** y seleccione **gestionar cuenta**.



2. En la ficha Miembros, seleccione el menú de acciones de la fila correspondiente al usuario.
3. Seleccione **desasociar usuario** y seleccione **desasociar** para confirmar.

Crear y administrar cuentas de servicio

Una cuenta de servicio actúa como un "usuario" que puede realizar llamadas API autorizadas a BlueXP con

fin de automatización. Esto facilita la gestión de la automatización, ya que no necesita crear scripts de automatización basados en la cuenta de usuario de una persona real que pueda salir de la empresa en cualquier momento.

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

Tenga en cuenta que un token de actualización no es necesario para las operaciones de API cuando se utiliza una cuenta de servicio. ["Obtenga más información sobre los tokens de actualización"](#)

Cree una cuenta de servicio

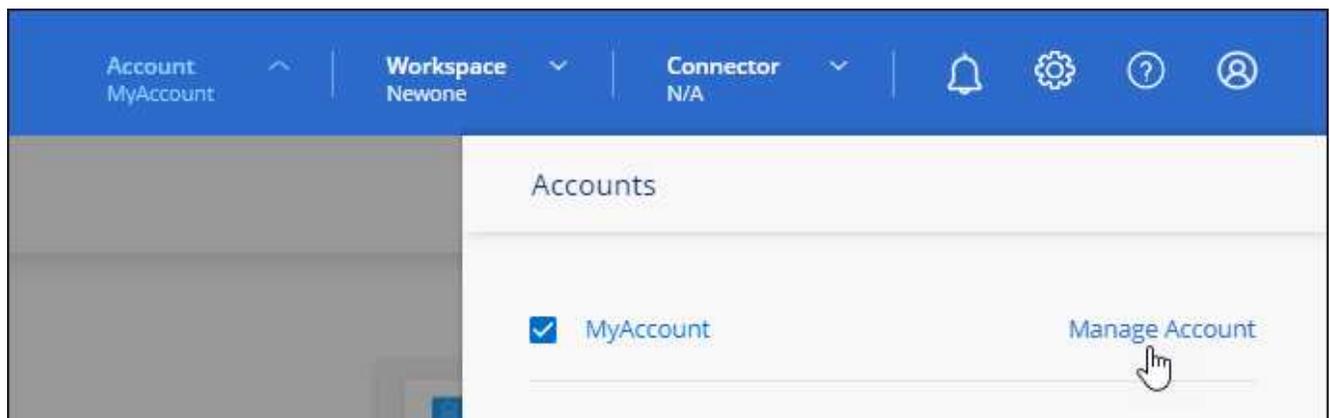
Cree tantas cuentas de servicio como necesite para gestionar los recursos en sus entornos de trabajo.

Pasos

1. En la parte superior de BlueXP, seleccione la lista desplegable **cuenta**.



2. Seleccione **Administrar cuenta** junto a la cuenta seleccionada actualmente.



3. En la ficha Miembros, seleccione **Crear cuenta de servicio**.
4. Introduzca un nombre.
5. Seleccione **Crear**.
6. Copie o descargue el ID del cliente y el secreto del cliente.

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

7. Seleccione **Cerrar**.

Obtener un token de portador para una cuenta de servicio

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

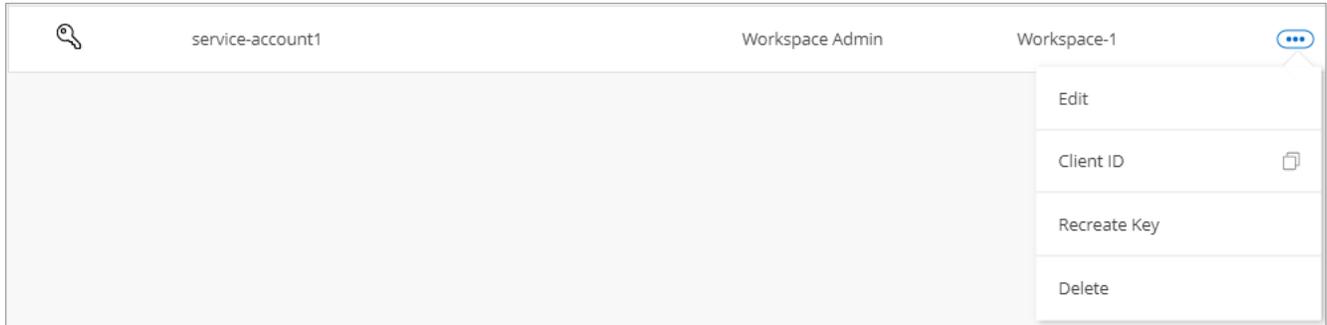
"Aprenda a crear un token de cuenta de servicio"

Copie el ID del cliente

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

Pasos

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



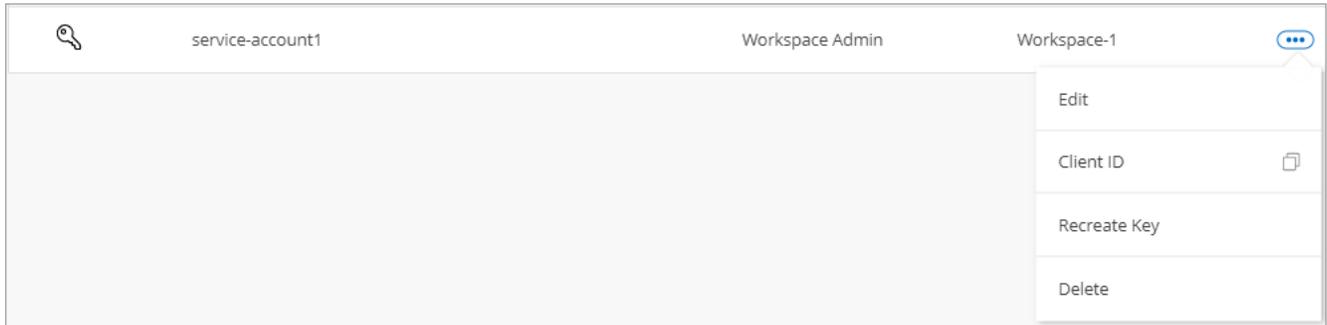
2. Seleccione **ID de cliente**.
3. El ID se copia en el portapapeles.

Vuelva a crear las claves

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

Pasos

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



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

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

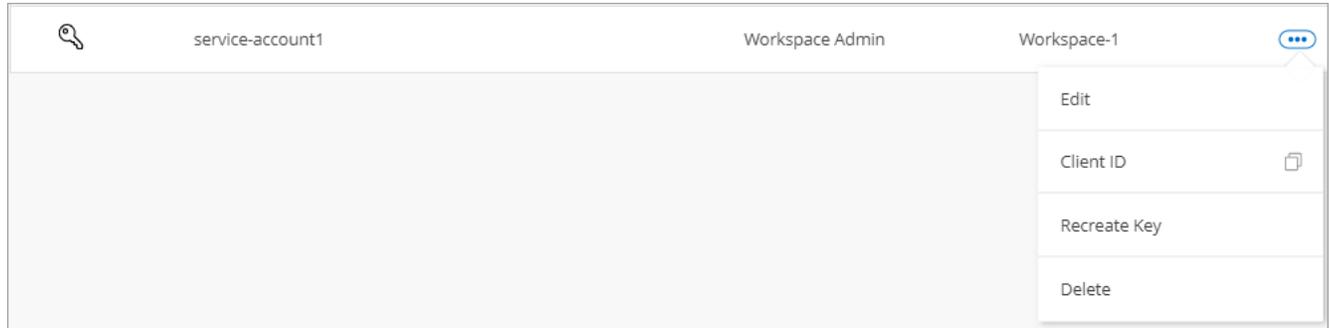
5. Seleccione **Cerrar**.

Eliminar una cuenta de servicio

Elimine una cuenta de servicio si ya no necesita utilizarla.

Pasos

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



2. Seleccione **Eliminar**.
3. Seleccione **Eliminar** de nuevo para confirmar.

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"](#)
- ["Analiza los datos de volúmenes de ONTAP on-premises con 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"](#)

Información de copyright

Copyright © 2025 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPTIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.