Comience con el modo privado

Setup and administration

NetApp
April 26, 2024

Tabla de contenidos

Comience con el modo privado

Flujo de trabajo inicial (modo privado)

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

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

Antes de empezar, debería comprender "Cuentas BlueXP", "Conectores", y. "modos de despliegue".

1 **"Prepárese para la puesta en marcha"**

1. Prepare un host de Linux dedicado que cumpla los requisitos de CPU, RAM, espacio en disco, Docker Engine y mucho más.
2. Configure las redes que proporcionen acceso a las redes de destino.
3. Para implementaciones en la nube, configure permisos en su proveedor de cloud para que pueda asociar dichos permisos con el conector después de instalar el software.

2 **"Despliegue el conector"**

1. Instale el software del conector en su propio host Linux.
2. Configure BlueXP abriendo un navegador Web e introduciendo la dirección IP del host Linux.
3. Para implementaciones en la nube, proporcione a BlueXP los permisos que configuró anteriormente.

Preparación para la implementación en modo privado

Prepara tu entorno antes de poner en marcha BlueXP en modo privado. Por ejemplo, debe revisar los requisitos del host, preparar redes, configurar permisos y mucho más.

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

Paso 1: Entender cómo funciona el modo privado

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

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

Además, no todos los servicios de BlueXP están disponibles.

"Aprenda cómo funciona el modo privado".

Paso 2: Revise las opciones de instalación

En modo privado, puede instalar el conector en las instalaciones o en la nube mediante la instalación manual del conector en su propio host Linux.

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.

Sistemas operativos compatibles

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

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

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

Hipervisor

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

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

CPU

4 núcleos o 4 vCPU

RAM

14 GB

Tipo de instancia de AWS EC2

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

Tamaño de la máquina virtual de Azure

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

Tipo de máquina de Google Cloud

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

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

Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

Motor Docker

Se requiere Docker Engine en el host antes de instalar Connector.

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

"Ver las instrucciones de instalación"

Paso 4: Prepare la red para el conector

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

Conexiones a redes de destino

El conector debe tener una conexión de red a la ubicación en la que desea gestionar el almacenamiento. Por ejemplo, el VPC o vnet donde planea poner en marcha Cloud Volumes ONTAP, o el centro de datos donde residen los clústeres de ONTAP en las instalaciones.

Extremos para operaciones del día a día

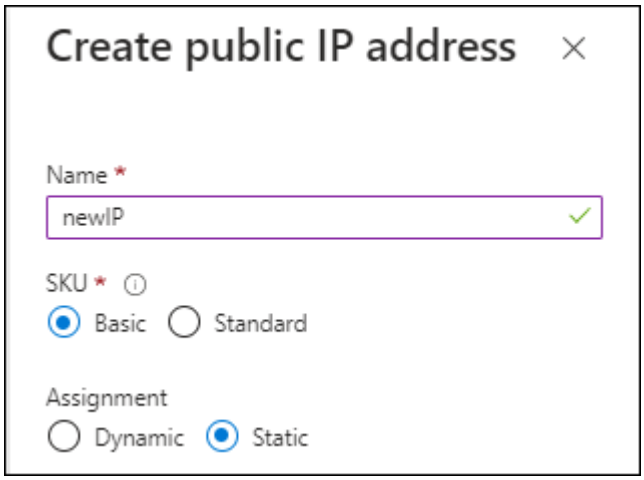
Connector se pone en contacto con los siguientes puntos finales para gestionar los recursos y procesos dentro de su entorno de nube pública.

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

Puntos finales	Específico
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

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

- Dirección IP
- Credenciales
- Certificado HTTPS

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

+
Con el modo privado, la única vez que BlueXP envía tráfico saliente es al proveedor de cloud para crear un sistema Cloud Volumes ONTAP.

Puertos

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

HTTP (80) y HTTPS (443) proporcionan acceso a la consola BlueXP. SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.

Habilite NTP

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

Paso 5: Preparar permisos en la nube

Si 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. Selecciona **Políticas > Crear política**.
   b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".
   c. Finalice los pasos restantes para crear la directiva.
3. Cree un rol IAM:
   a. Selecciona **Roles > Crear rol**.
   b. Seleccione **Servicio AWS > EC2**.
   c. Agregue permisos asociando la directiva que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

Resultado

Ahora tiene un rol de IAM para la instancia de Connector EC2.

Clave de acceso de AWS

Configurar permisos y una clave de acceso para un usuario de IAM. Deberá proporcionar a BlueXP la clave de acceso de AWS después de instalar el conector y configurar BlueXP.

Pasos

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

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

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

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

Resultado

La cuenta ahora tiene los permisos necesarios.

Rol de Azure

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

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

Pasos

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

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

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

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

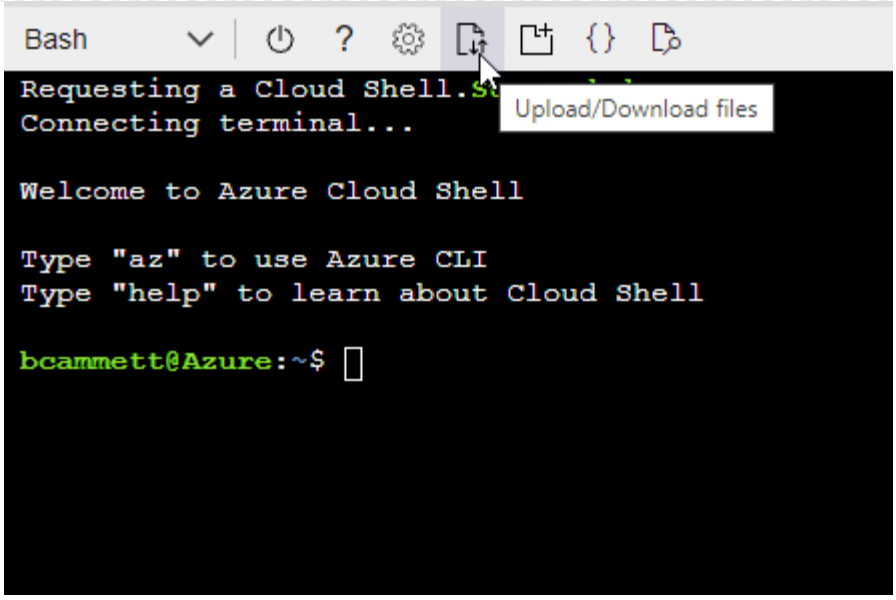
   ejemplo

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

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

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

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



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

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

Resultado

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

Servicio principal de Azure

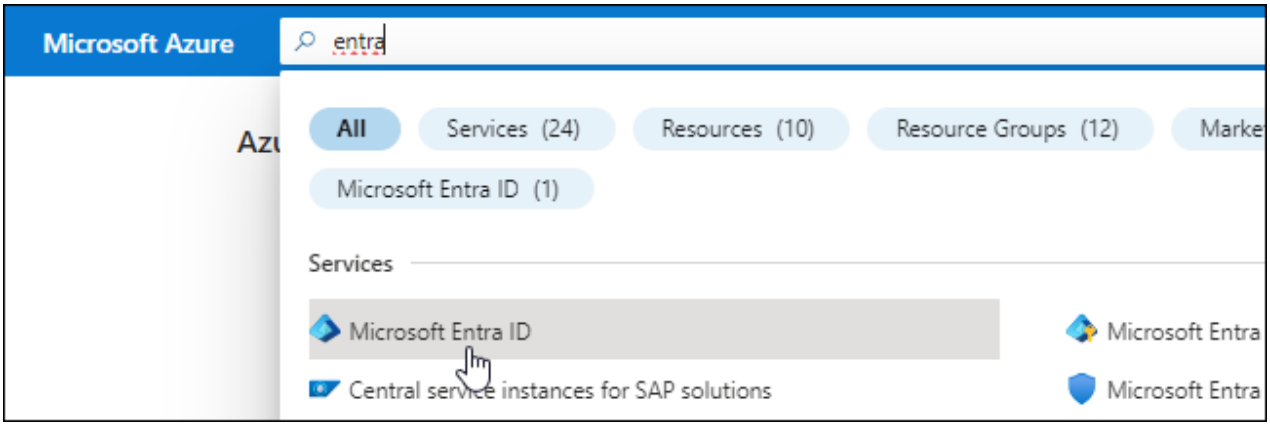
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita. Necesitará proporcionar estas credenciales a BlueXP después de instalar el conector y configurar BlueXP.

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

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

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

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



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

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

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

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

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

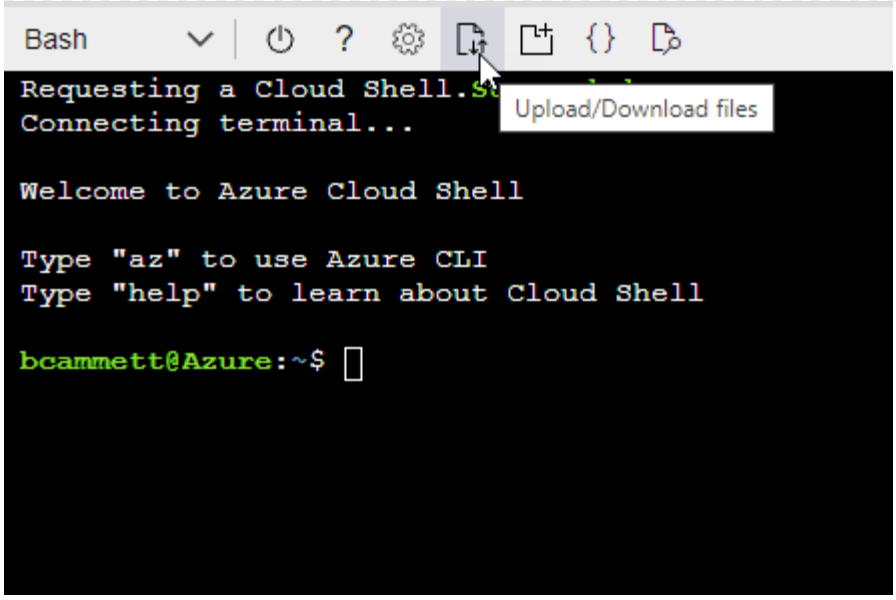
      ejemplo

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

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

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

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



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

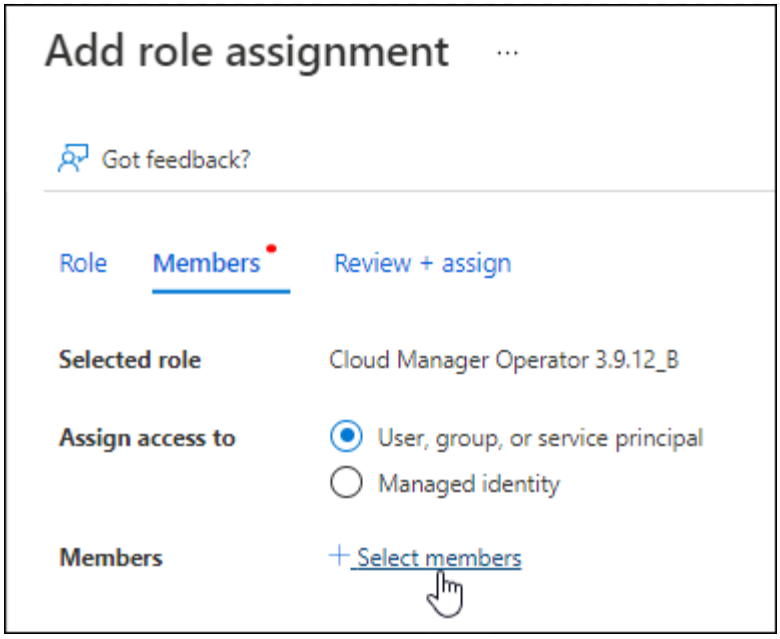
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

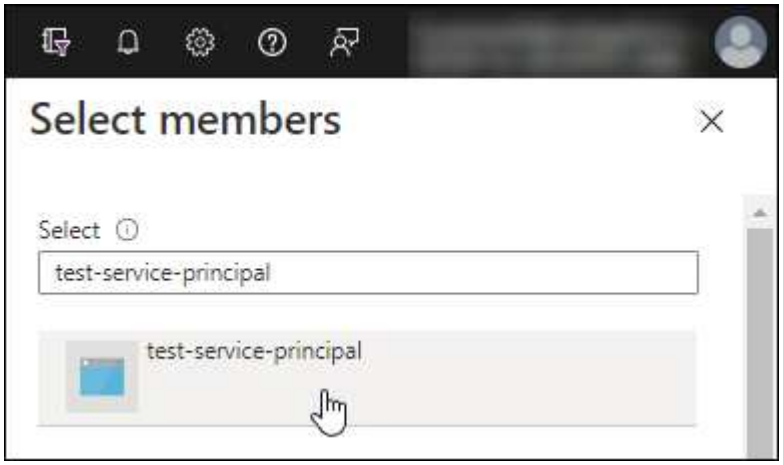
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**,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

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



- Busque el nombre de la aplicación.

  Veamos un ejemplo:



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

f. Seleccione **revisar + asignar**.

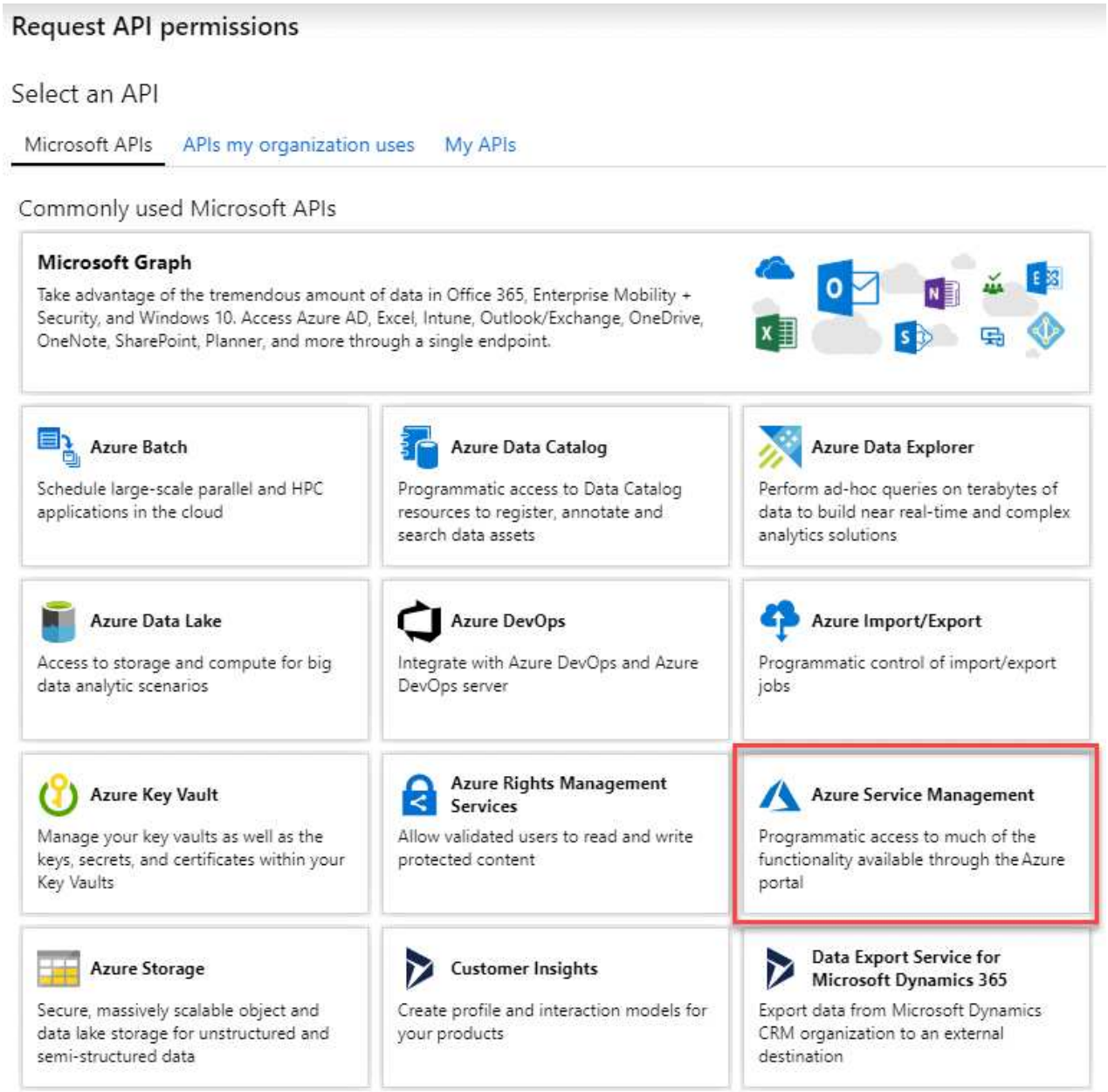
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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

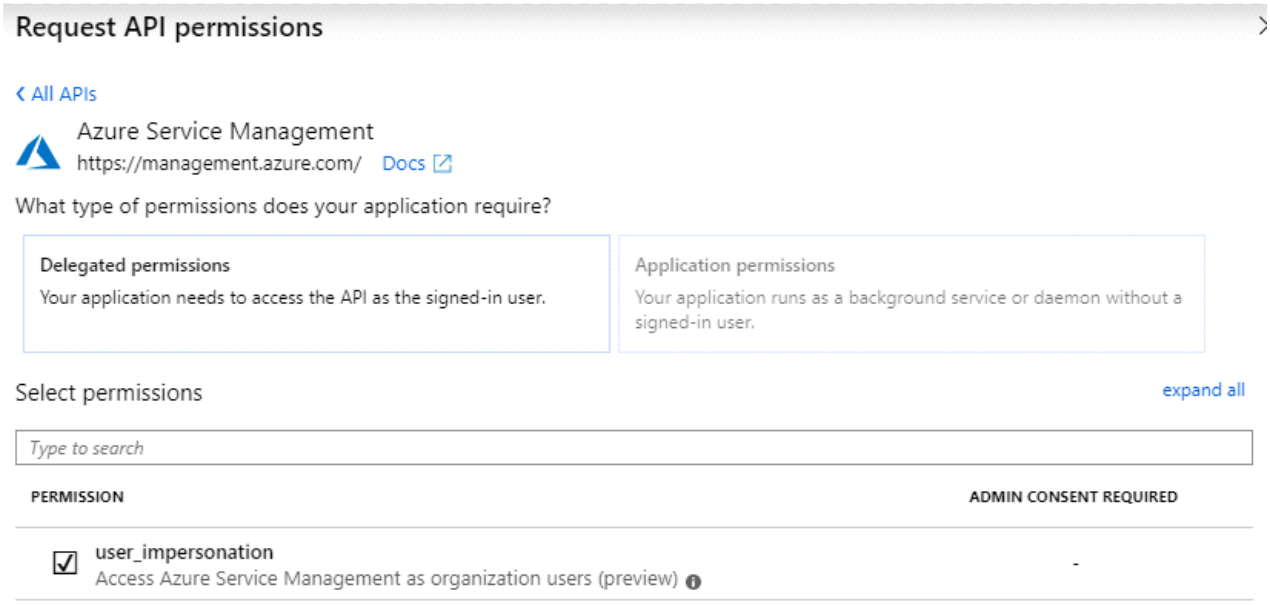
Añada permisos de API de administración de servicios de Windows Azure

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

3. En **API de Microsoft**, seleccione **Administración de servicios Azure**.

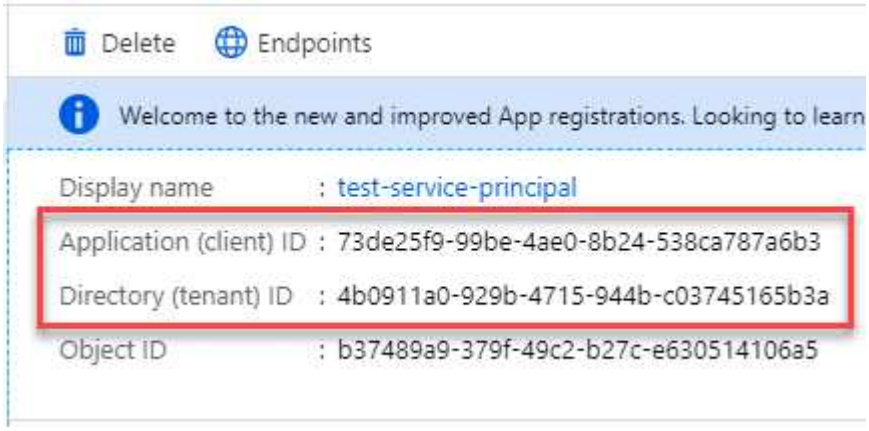


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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

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



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

Cree un secreto de cliente

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

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

Resultado

Su principal de servicio ahora está configurado y debe haber copiado el ID de aplicación (cliente), el ID de directorio (arrendatario) y el valor del secreto de cliente. Necesita introducir esta información en BlueXP cuando agrega una cuenta de Azure.

Cuenta de servicio de Google Cloud

Cree una función y aplíquela a una cuenta de servicio que utilizará para la instancia de Connector VM.

Pasos

1. Cree un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya los permisos definidos en "Política de conectores para Google Cloud".

   b. Desde Google Cloud, active Cloud Shell.

   c. Cargue el archivo YAML que incluye los permisos necesarios para el conector.

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

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

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

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

2. Cree una cuenta de servicio en Google Cloud:

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

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

   c. Seleccione la función que acaba de crear.

   d. Finalice los pasos restantes para crear la función.

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

Resultado

Ahora tiene una cuenta de servicio que puede asignar a la instancia de Connector VM.

Paso 6: Habilita las API de Google Cloud

Se necesitan varias API para poner en marcha Cloud Volumes ONTAP en Google Cloud.

Paso

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

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

Despliegue el conector en modo privado

Pon en marcha el conector en modo privado para poder utilizar BlueXP sin conectividad saliente a la capa de BlueXP SaaS. Para comenzar, instala el Connector, configura BlueXP accediendo a la interfaz de usuario que se ejecuta en el Connector y, a continuación, proporciona los permisos de nube que hayas configurado previamente.

Paso 1: Instale el conector

Descargue el instalador del producto desde el sitio de soporte de NetApp y, a continuación, instale manualmente el conector en su propio host Linux.

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

Antes de empezar

Se requieren privilegios de usuario raíz para instalar el conector.

Pasos

1. Compruebe que docker está activado y en ejecución.

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

2. Descargue el software del conector de "Sitio de soporte de NetApp"

   Asegúrese de descargar el instalador fuera de línea para redes privadas sin acceso a Internet.

3. Copie el instalador en el host Linux.
4. Asigne permisos para ejecutar el script.

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

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

5. Ejecute el script de instalación:

```
sudo /path/BlueXP-Connector-offline-<version>
```

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

Resultado

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

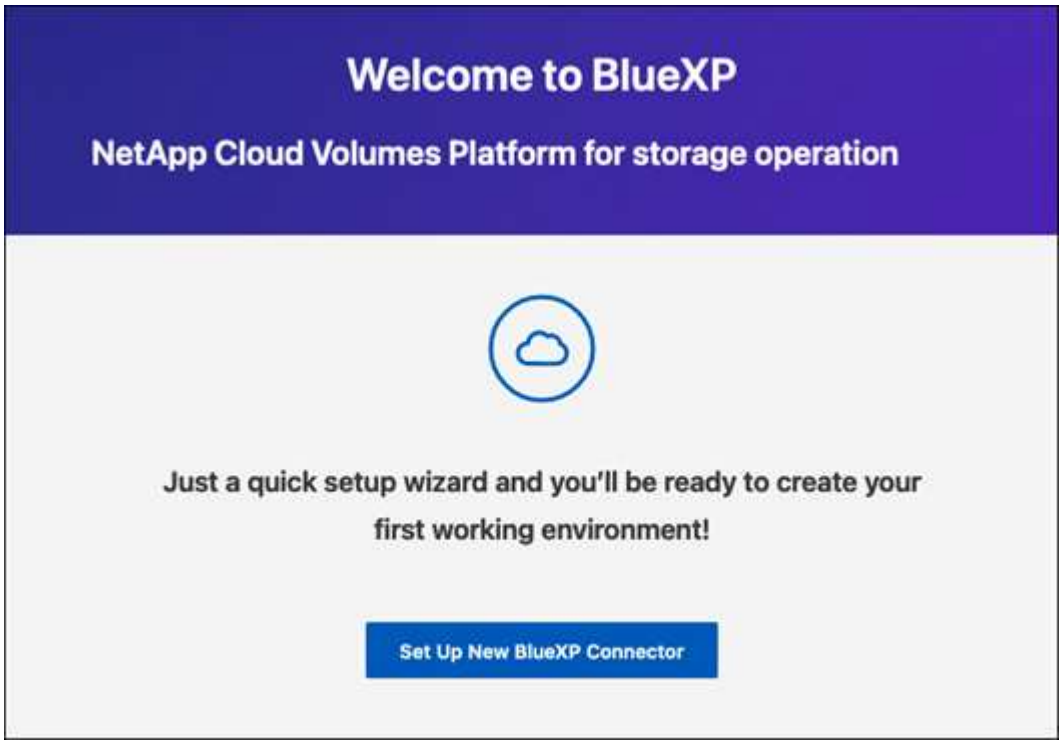
Paso 2: Configura BlueXP

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

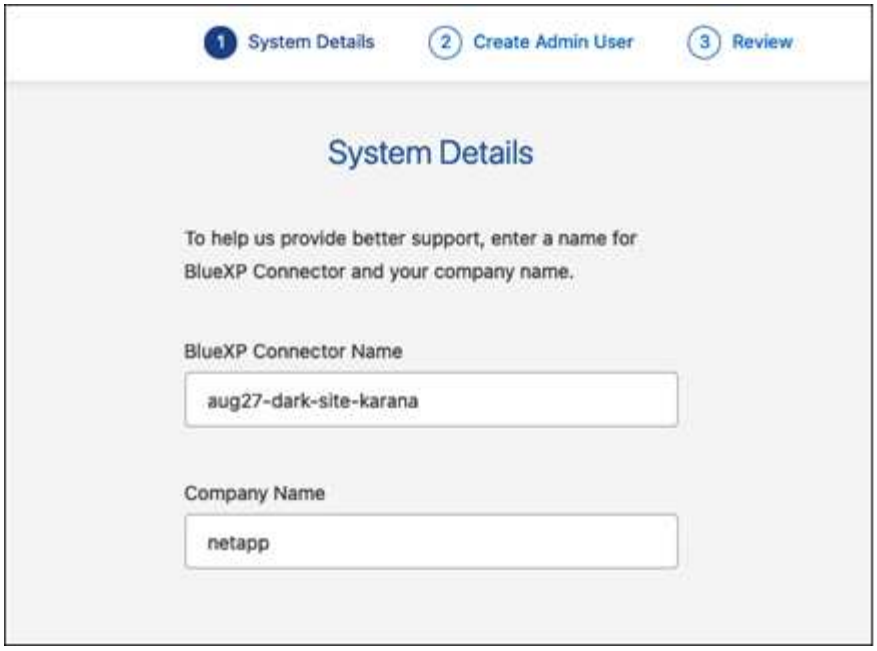
Pasos

1. Abra un explorador web e introduzca https://ipaddress Donde ipaddress es la dirección IP del host Linux en el que instaló el conector.

   Debe ver la siguiente pantalla.



2. Selecciona **Configurar nuevo conector BlueXP** y sigue las indicaciones para configurar el sistema.
   - **Detalles del sistema**: Introduzca un nombre para el conector y el nombre de su empresa.



- **Crear un usuario administrador**: Crea el usuario administrador para el sistema.

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

- **Revisión**: Revisa los detalles, acepta el contrato de licencia y luego selecciona **Configurar**.

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

Resultado

El conector ahora está instalado y configurado.

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

El futuro

Proporcione a BlueXP los permisos que configuró anteriormente.

Paso 3: Proporcionar permisos a BlueXP

Si desea crear entornos de trabajo de Cloud Volumes ONTAP, tendrá que proporcionar a BlueXP los permisos de cloud que configuró anteriormente.

"Aprenda cómo preparar los permisos en el cloud".

Rol IAM de AWS

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

Pasos

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

Resultado

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

Clave de acceso de AWS

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

Pasos

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

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

Resultado

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

Rol de Azure

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

Pasos

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

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

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

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

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

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

Resultado

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

Servicio principal de Azure

Proporcione a BlueXP las credenciales para la entidad de servicio de Azure que configuró anteriormente.

Pasos

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

2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.
   b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:
      - ID de aplicación (cliente)
      - ID de directorio (inquilino)
      - Secreto de cliente
   c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.
   d. **Revisión**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

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

Cuenta de servicio de Google Cloud

Asocie la cuenta de servicio a la máquina virtual del conector.

Pasos

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

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

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

Resultado

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

Qué puede hacer después (modo privado)

Después de empezar a utilizar BlueXP en modo privado, puede empezar a utilizar los servicios BlueXP compatibles con modo privado.

Si necesita ayuda, consulte la siguiente documentación:

- "Creación de sistemas Cloud Volumes ONTAP"
- "Detectar clústeres de ONTAP en las instalaciones"
- "Replicar datos"
- "Analiza los datos de volúmenes de ONTAP on-premises con la clasificación de BlueXP"
- "Haz un backup de los datos de volúmenes de ONTAP en las instalaciones en StorageGRID mediante el backup y la recuperación de BlueXP"

Enlace relacionado

"Modos de implementación de BlueXP"