Comience con el modo restringido

BlueXP setup and administration

NetApp
September 09, 2024

Tabla de contenidos

Comience con el modo restringido . . . 1
- Flujo de trabajo inicial (modo restringido) . . . 1
- Preparación para la puesta en marcha en modo restringido . . . 1
- Despliegue el conector en modo restringido . . . 20
- Suscribirse a BlueXP (modo restringido) . . . 32
- Qué puede hacer después (modo restringido) . . . 38

Comience con el modo restringido

Flujo de trabajo inicial (modo restringido)

Empieza a usar BlueXP en modo restringido preparando tu entorno, poniendo en marcha Connector y suscribiéndote a BlueXP.

El modo restringido suele ser utilizado por los gobiernos estatales y locales y las empresas reguladas, incluidas las implementaciones en las regiones AWS GovCloud y Azure Government. Antes de empezar, debería comprender "Cuentas BlueXP", "Conectores", y. "modos de despliegue".

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

1. Prepare un host 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.

2 **"Despliegue el conector"**

1. Instale el conector desde el mercado de su proveedor de cloud o instalando manualmente el software en su propio host Linux.
2. Configure BlueXP abriendo un navegador Web e introduciendo la dirección IP del host Linux.
3. Proporcione a BlueXP los permisos que configuró anteriormente.

3 **"Suscríbase a BlueXP"**

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

Preparación para la puesta en marcha en modo restringido

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

Paso 1: Entender cómo funciona el modo restringido

Antes de empezar, debe tener una comprensión de cómo funciona BlueXP en modo restringido.

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

Además, no todos los servicios de BlueXP están disponibles.

"Descubra cómo funciona el modo restringido".

Paso 2: Revise las opciones de instalación

En el modo restringido, sólo puede instalar el conector en la nube. Están disponibles las siguientes opciones de instalación:

- Desde el AWS Marketplace
- Desde Azure Marketplace
- Instalación manual del conector en su propio host Linux que se ejecuta en AWS, Azure o Google Cloud

Paso 3: Revise los requisitos del host

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

Al poner en marcha el conector desde AWS o Azure Marketplace, la imagen incluye el sistema operativo y los componentes de software necesarios. Simplemente tiene que elegir un tipo de instancia que cumpla con los requisitos de CPU y RAM.

Host dedicado

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

Sistemas operativos compatibles

- Sistema operativo Ubuntu 22,04 LTS
- Red Hat Enterprise Linux
  - 8,6 a 8,10
  - 9,1 a 9,4

    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 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.

Herramienta de orquestación de contenedores

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

- Se requiere Podman para Red Hat Enterprise Linux.

  Se deben cumplir los siguientes requisitos previos para Podman:

  - Se requiere la versión 4.6.1 o 4.9.4 de Podman
  - 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
- Se requiere Docker Engine para Ubuntu.
  - La versión mínima admitida es 23,0.6.
  - La versión máxima admitida es 26,0.0.

    Tenga en cuenta que Docker Engine 26 es compatible con instalaciones de conector *new* a partir de la versión 3.9.44 del conector.

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.

- Se requiere Docker Engine para Ubuntu.

Ejemplo 1. Pasos

Podman

Instale una versión compatible de Podman. Ver las versiones de Podman que admite BlueXP .

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

Instale una versión compatible de Docker Engine. Vea las versiones de Docker Engine compatibles con BlueXP .

Pasos

1. Instale Docker Engine.

   "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://signin.b2c.netapp.com	Se requiere actualizar las credenciales del sitio de soporte de NetApp (NSS) o añadir nuevas credenciales de NSS a BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	El explorador Web se conecta a estos extremos para una autenticación de usuario centralizada a través de BlueXP.
https://widget.intercom.io	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

Puntos finales contactados durante la instalación manual

Al instalar manualmente el conector en su propio host Linux, el instalador del conector requiere acceso a las siguientes direcciones URL durante el proceso de instalación:

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Este punto final no es necesario en las regiones gubernamentales de Azure.

- https://occmclientinfragov.azurecr.us

  Este extremo solo se requiere en las regiones gubernamentales de Azure.

Es posible que el host intente actualizar paquetes de sistema operativo durante la instalación. El host puede ponerse en contacto con diferentes sitios de duplicación para estos paquetes de SO.

Acceso a Internet saliente para operaciones diarias

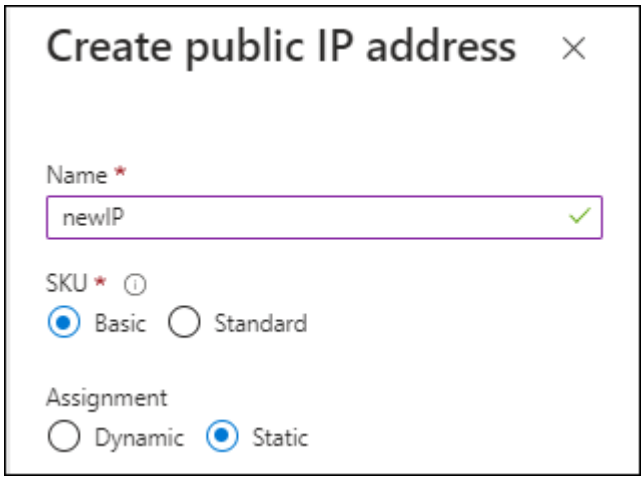
La ubicación de red en la que implemente el conector debe tener una conexión a Internet saliente. El conector requiere acceso saliente a Internet para ponerse en contacto con los siguientes extremos con el fin de gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	Para gestionar recursos en regiones gubernamentales de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Para gestionar recursos en Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.

Puntos finales	Específico
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP. Tenga en cuenta que el conector se está poniendo en contacto con «cloudmanager.cloud.netapp.com "», pero comenzará a ponerse en contacto con «api.bluexp.netapp.com" en una próxima versión.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Este punto final no es necesario en las regiones gubernamentales de Azure. https://occmclientinfragov.azurecr.us Este extremo solo se requiere en las regiones gubernamentales de Azure.	Para actualizar el conector y sus componentes de Docker.

La dirección IP pública en Azure

Si desea utilizar una dirección IP pública con Connector VM en Azure, la dirección IP debe utilizar una SKU básica para garantizar que BlueXP utilice esta dirección IP pública.



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

"Documentación para Azure: SKU de IP pública"

Servidor proxy

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

- 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.

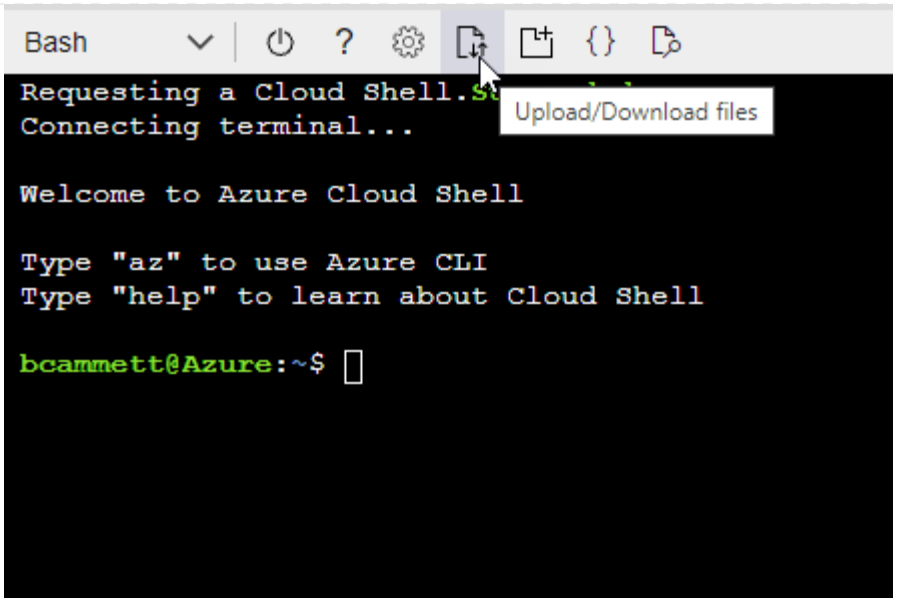
   ejemplo

   ```
   "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

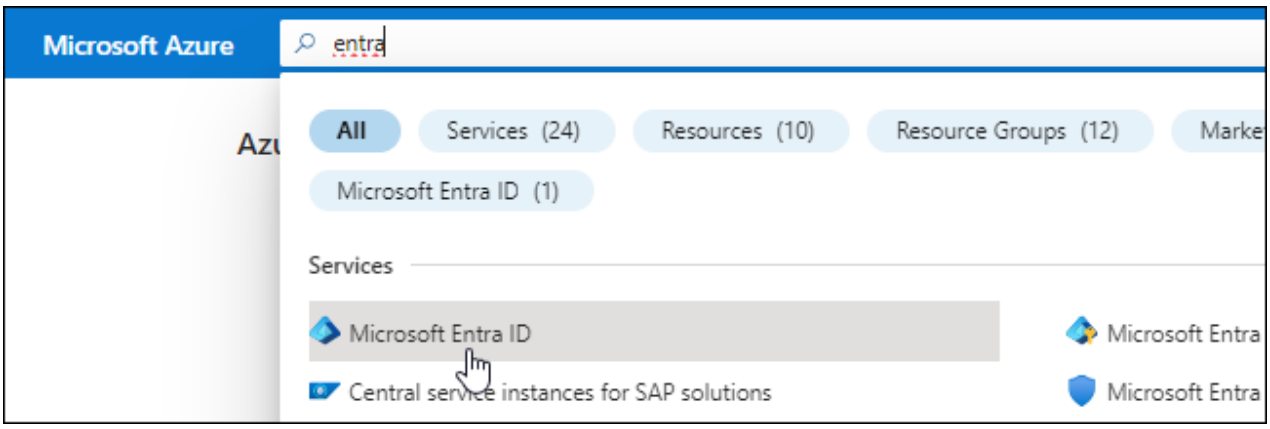
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita. Necesitará proporcionar estas credenciales a BlueXP después de instalar el conector y configurar BlueXP.

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.

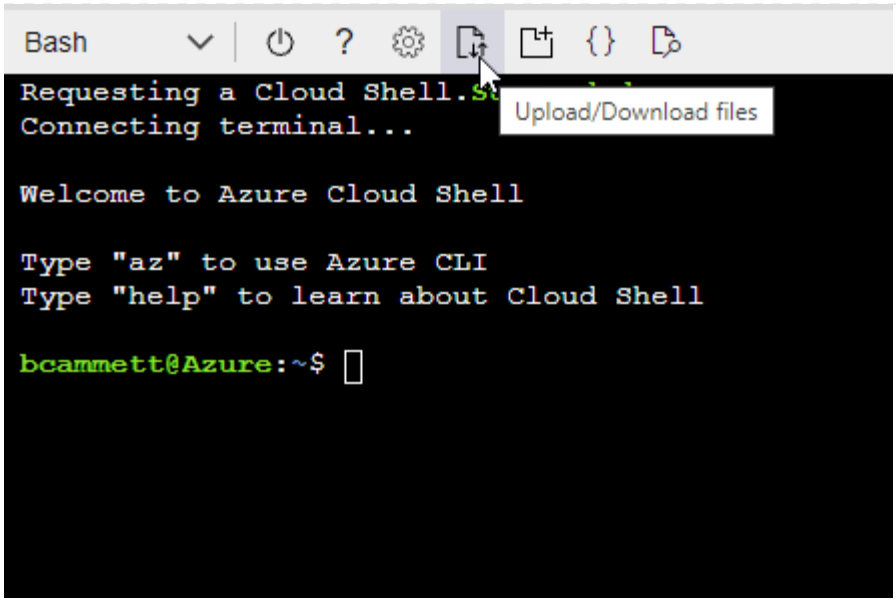
      ejemplo

      ```
      "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:

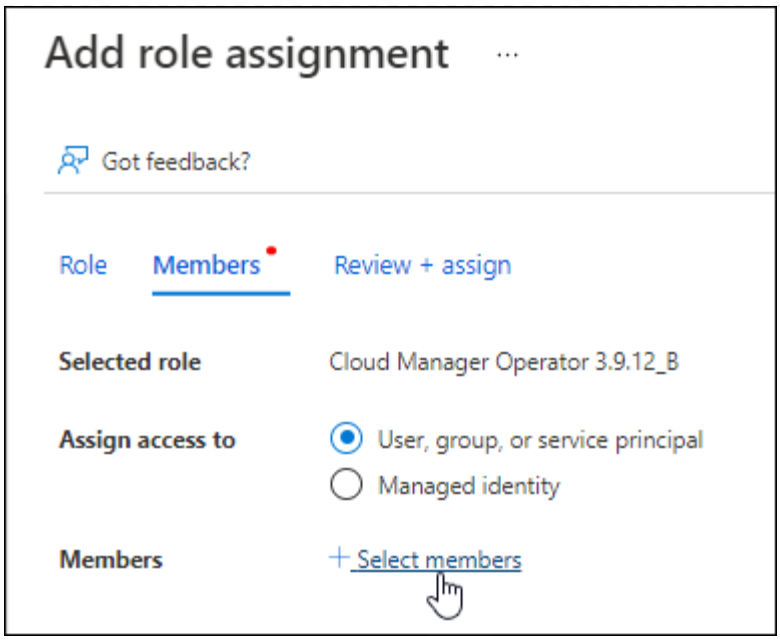
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

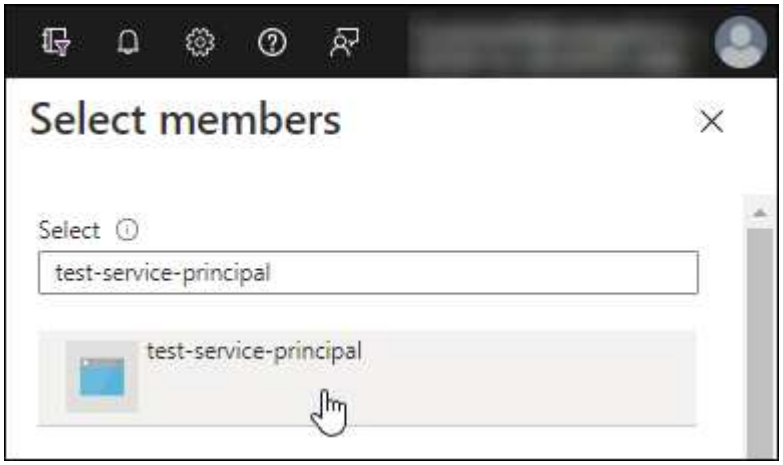
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**,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

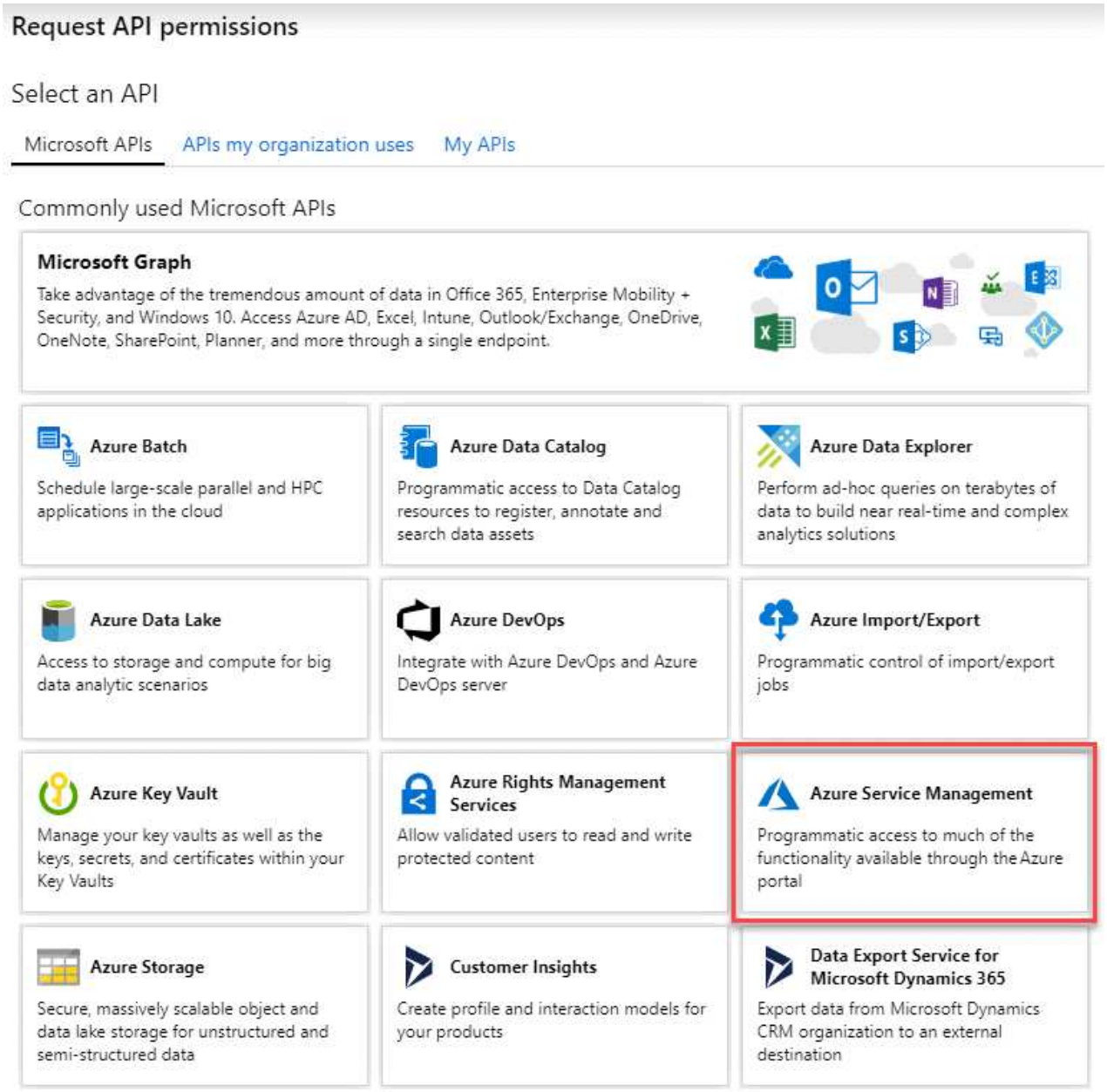
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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.

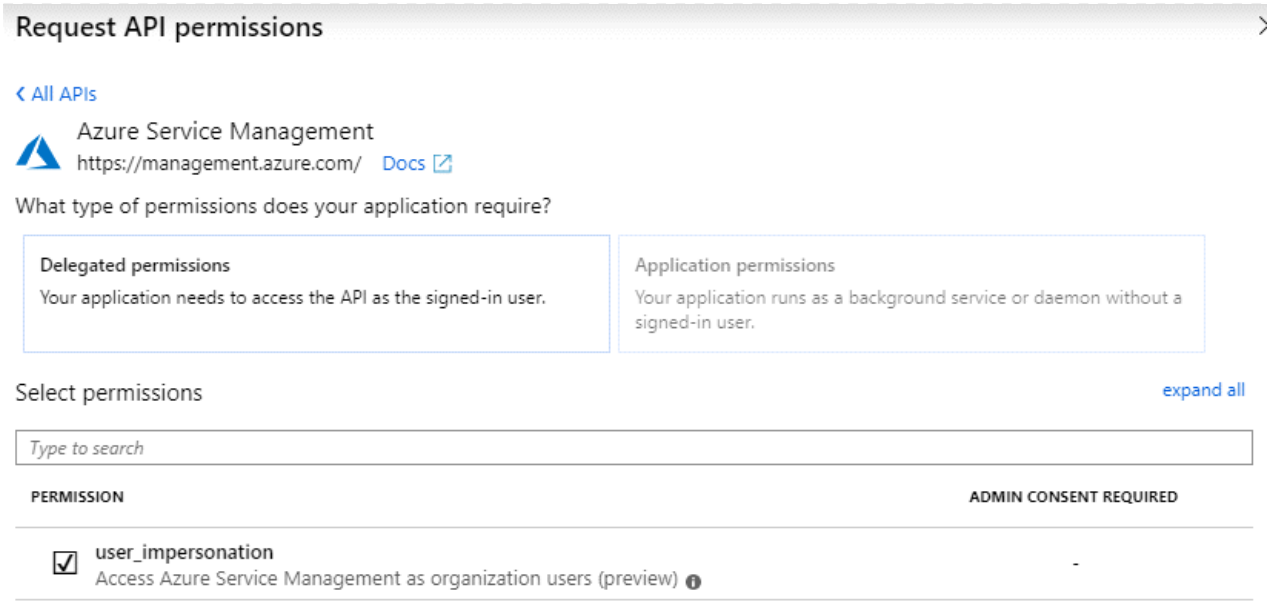
Añada permisos de API de administración de servicios de Windows Azure

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**.

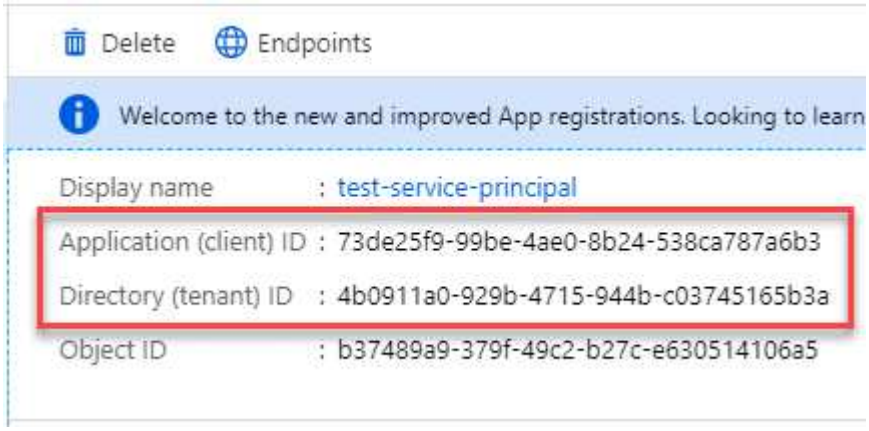


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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

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

Paso 1: Instale el conector

Instale el conector desde el mercado de su proveedor de cloud o instalando manualmente el software en su propio host Linux.

Mercado comercial AWS

Antes de empezar

Debe tener lo siguiente:

- Un VPC y una subred que cumplan los requisitos de red.

  "Obtenga información sobre los requisitos de red"

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

  "Aprenda a configurar los permisos de AWS"

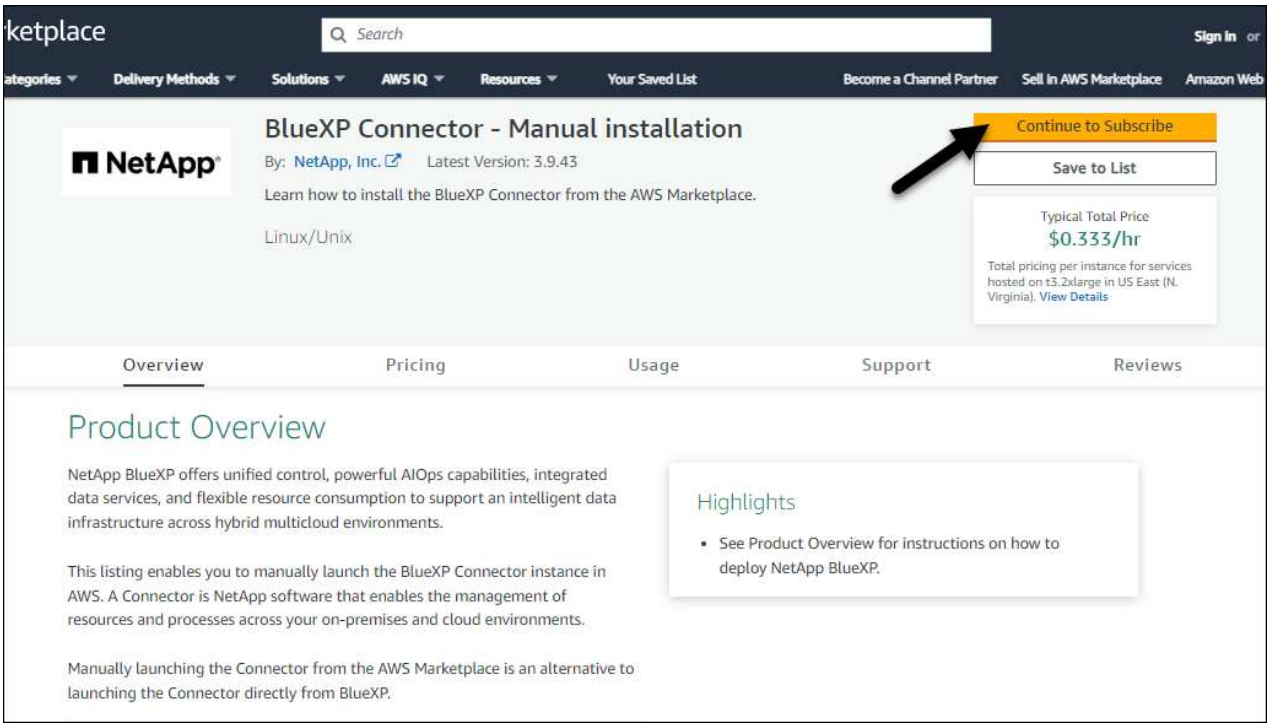
- Permisos para suscribirse y cancelar la suscripción a AWS Marketplace para su usuario de IAM.
- Comprensión de los requisitos de CPU y RAM para la instancia.

  "Revisar requisitos de instancia".

- Una pareja de claves para la instancia de EC2.

Pasos

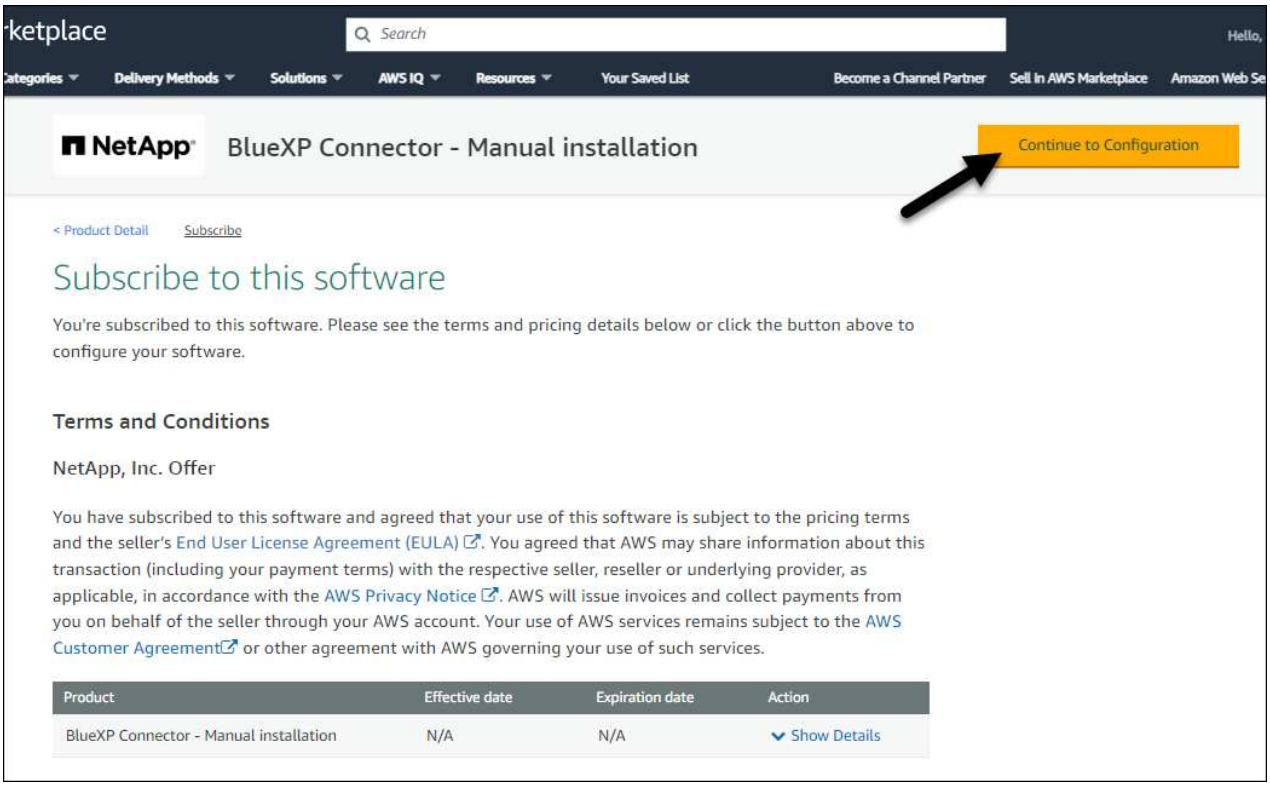
1. Vaya a la "Lista del conector BlueXP en el AWS Marketplace"
2. En la página de Marketplace, selecciona **Continuar para suscribirte**.



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"

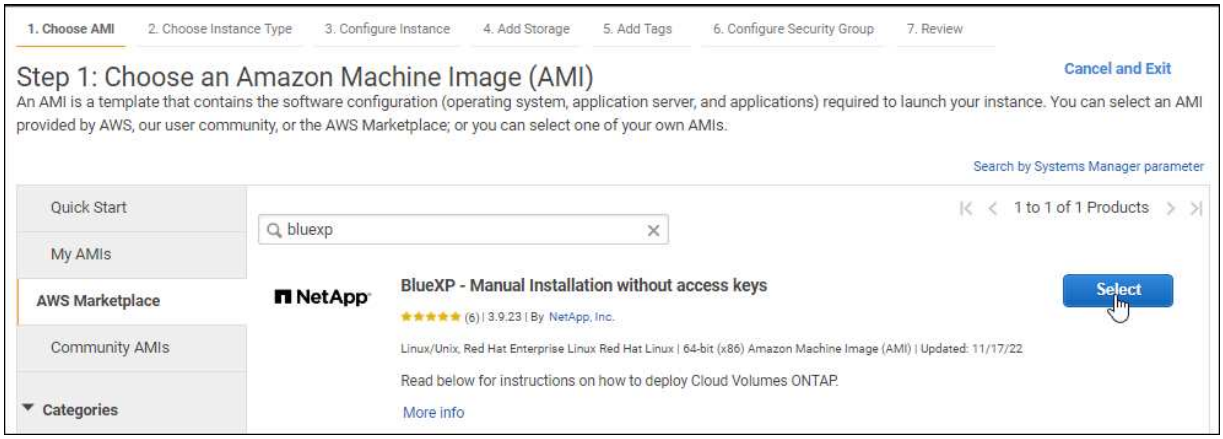
- Función IAM con una directiva adjunta que incluye los permisos necesarios para el conector.

  "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.

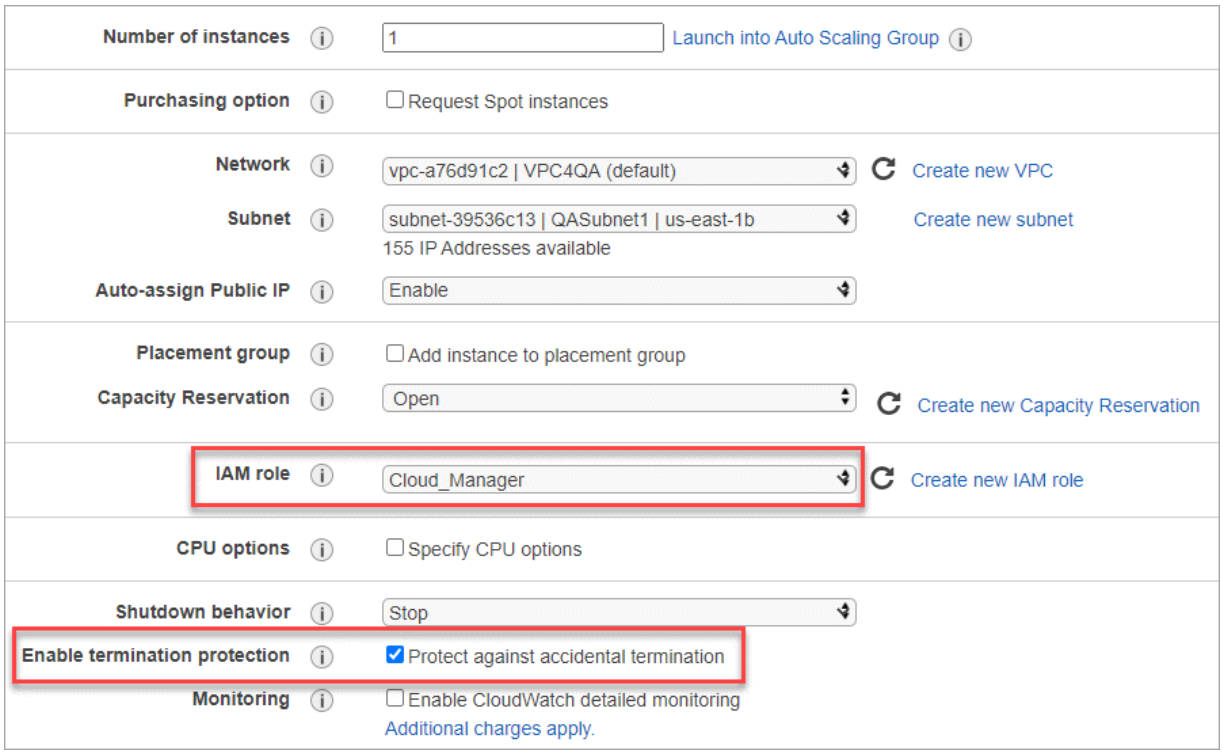


   d. Seleccione **continuar**.
2. Siga las instrucciones para configurar y desplegar la instancia:

- **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.

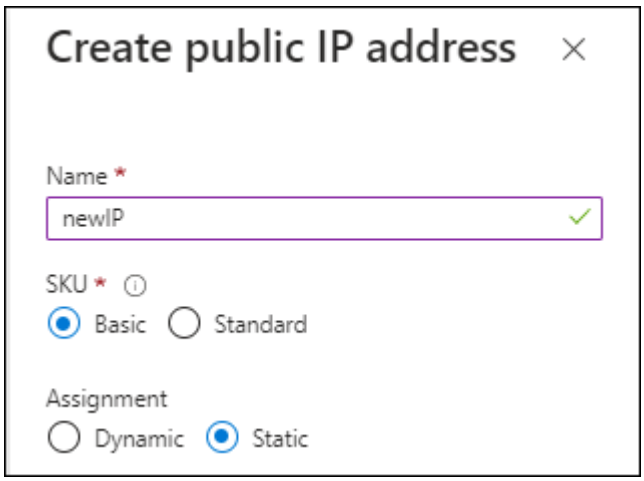
  "Aprenda a configurar los permisos de Azure"

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.

  Tenga en cuenta que BlueXP no es compatible con los servidores proxy transparentes.
- Un certificado firmado por CA, si el servidor proxy utiliza HTTPS o si el proxy es un proxy de interceptación.
- 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>
```

Los parámetros --proxy y --cacert son opcionales. Si tiene un servidor proxy, deberá introducir los parámetros como se muestra. El instalador no le solicita que proporcione información sobre un proxy.

A continuación encontrará un ejemplo del comando utilizando los dos parámetros opcionales:

```
 ./BlueXP-Connector-Cloud-v3.9.40--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 sólo es obligatorio si se especifica un servidor proxy HTTPS o si el proxy es un proxy de interceptación.

Resultado

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

El futuro

Configure BlueXP.

Paso 2: Configura BlueXP

Cuando acceda a la consola BlueXP por primera vez, se le solicitará que elija una cuenta para asociar el conector y tendrá que activar el modo restringido.

Si ya tiene una cuenta y desea crear otra, debe utilizar la API de soporte. "Aprenda a crear una cuenta de BlueXP adicional".

Pasos

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

   https://ipaddress

2. Regístrese o inicie sesión en BlueXP.
3. Después de iniciar sesión, configure BlueXP:

   a. Introduzca un nombre para el conector.

   b. Introduzca un nombre para una nueva cuenta de BlueXP o seleccione una cuenta existente.

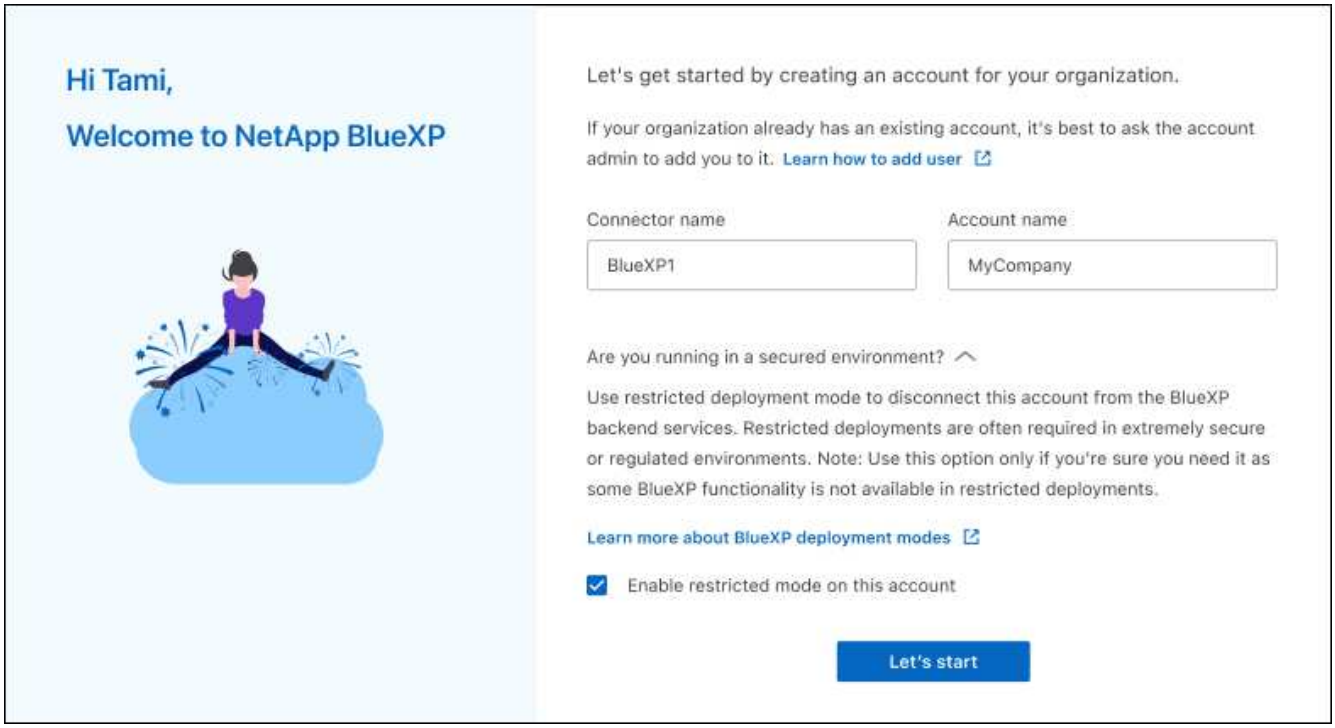
      Puede seleccionar una cuenta existente si su inicio de sesión ya está asociado con una cuenta de BlueXP.

   c. Seleccione **¿está ejecutando en un entorno protegido?**

   d. Seleccione **Activar modo restringido en esta cuenta**.

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

      Si ha desplegado el conector en una región gubernamental, la casilla de verificación ya está activada y no se puede cambiar. Esto se debe a que el modo restringido es el único modo compatible con las regiones gubernamentales.



a. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y configurado con su cuenta BlueXP. Todos los usuarios deben acceder a BlueXP mediante la dirección IP de la instancia de Connector.

El futuro

Proporcione a BlueXP los permisos que configuró anteriormente.

Paso 3: Proporcionar permisos a BlueXP

Si implementó el conector desde Azure Marketplace o si instaló manualmente el software Connector, debe proporcionar los permisos que configuró anteriormente para poder utilizar los servicios de BlueXP.

Estos pasos no se aplican si ha implementado el conector desde AWS Marketplace porque ha elegido el rol de IAM necesario durante la implementación.

"Aprenda cómo preparar los permisos en el cloud".

Rol IAM de AWS

Conecte el rol IAM que ha creado previamente a la instancia de EC2 donde ha instalado Connector.

Estos pasos sólo se aplican si instaló manualmente el conector en AWS. En el caso de implementaciones de AWS Marketplace, ya ha asociado la instancia del conector con una función IAM que incluye los permisos necesarios.

Pasos

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

Resultado

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

Clave de acceso de AWS

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

Pasos

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

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

Resultado

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

Rol de Azure

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

Pasos

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

   Es importante asignar el rol desde el servicio **Suscripciones** porque especifica el alcance de la

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

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

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

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

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

Resultado

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

Servicio principal de Azure

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

Pasos

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

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

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

Resultado

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

Cuenta de servicio de Google Cloud

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

Pasos

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

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

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

Resultado

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

Suscribirse a BlueXP (modo restringido)

Suscríbase a BlueXP en el mercado de su proveedor de la nube para pagar los servicios de BlueXP a una tarifa por hora (PAYGO) o a través de un contrato anual. Si adquirió una licencia de NetApp (BYOL), también deberá suscribirse a la oferta de mercado. Su licencia siempre se cobra primero, pero se le cobrará la tarifa por hora si excede la capacidad de su licencia o si el plazo de la licencia expira.

Una suscripción al mercado permite cargar los siguientes servicios de BlueXP con modo restringido:

- Backup y recuperación
- Clasificación
- Cloud Volumes ONTAP

Antes de empezar

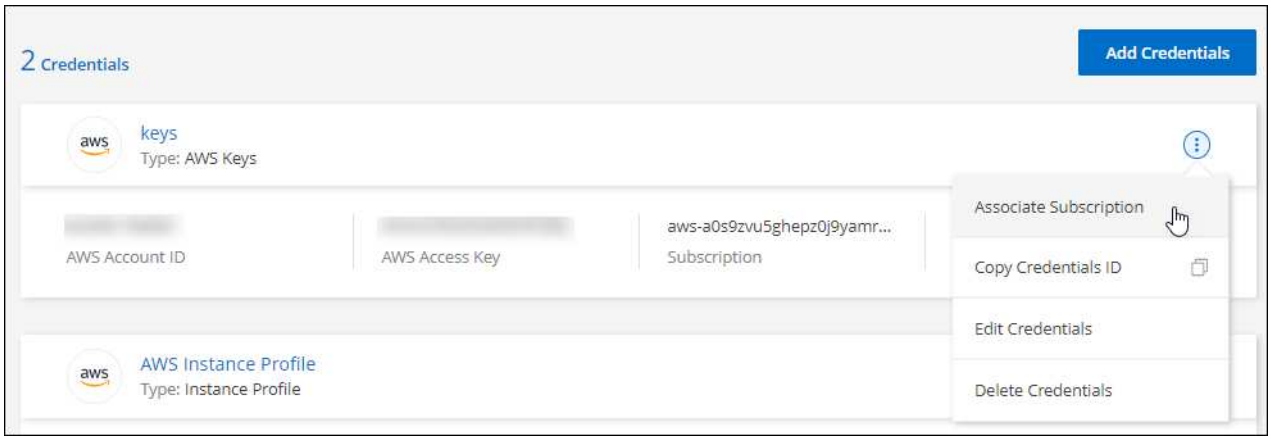
La suscripción a BlueXP implica asociar una suscripción al mercado con las credenciales de la nube asociadas con un conector. Si ha seguido el flujo de trabajo de inicio con modo restringido, ya debe tener un conector. Para obtener más información, consulte la "Inicio rápido para BlueXP en modo restringido".

AWS

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y seleccione **asociado**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos del AWS Marketplace:

   a. Seleccione **Ver opciones de compra**.

   b. Seleccione **Suscribirse**.

   c. Seleccione **Configurar su cuenta**.

      Se le redirigirá al sitio web de BlueXP.

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

      - Seleccione las cuentas de BlueXP con las que desea asociar esta suscripción.
      - En el campo **sustituir suscripción existente**, elija si desea sustituir automáticamente la suscripción existente para una cuenta con esta nueva suscripción.

        BlueXP reemplaza la suscripción existente para todas las credenciales de la cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

   Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

      - Seleccione **Guardar**.

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

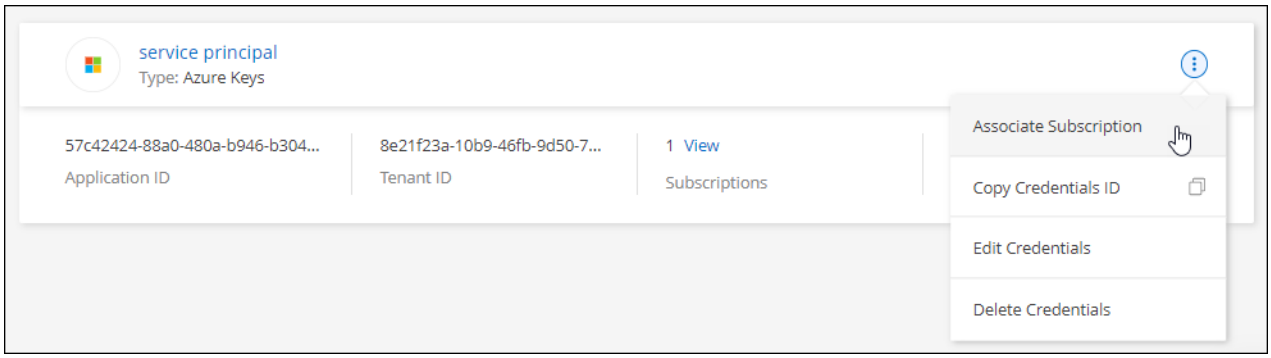
Suscríbete a BlueXP desde AWS Marketplace

Azure

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.

   Debe seleccionar las credenciales asociadas a un conector. No puedes asociar una suscripción al mercado con credenciales asociadas a BlueXP.



3. Para asociar las credenciales a una suscripción existente, seleccione la suscripción en la lista desplegable y seleccione **asociado**.
4. Para asociar las credenciales a una nueva suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos de Azure Marketplace:

   a. Si se le solicita, inicie sesión en su cuenta de Azure.

   b. Seleccione **Suscribirse**.

   c. Rellene el formulario y seleccione **Suscribirse**.

   d. Una vez completado el proceso de suscripción, seleccione **Configurar cuenta ahora**.

      Se le redirigirá al sitio web de BlueXP.

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

      - Seleccione las cuentas de BlueXP con las que desea asociar esta suscripción.
      - En el campo **sustituir suscripción existente**, elija si desea sustituir automáticamente la suscripción existente para una cuenta con esta nueva suscripción.

        BlueXP reemplaza la suscripción existente para todas las credenciales de la cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

   Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

      - Seleccione **Guardar**.

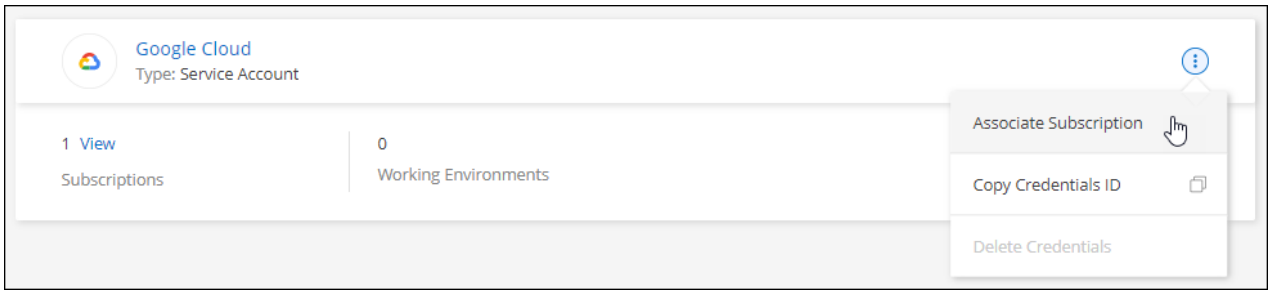
        En el siguiente vídeo se muestran los pasos para suscribirse desde Azure Marketplace:

   Suscríbete a BlueXP desde Azure Marketplace

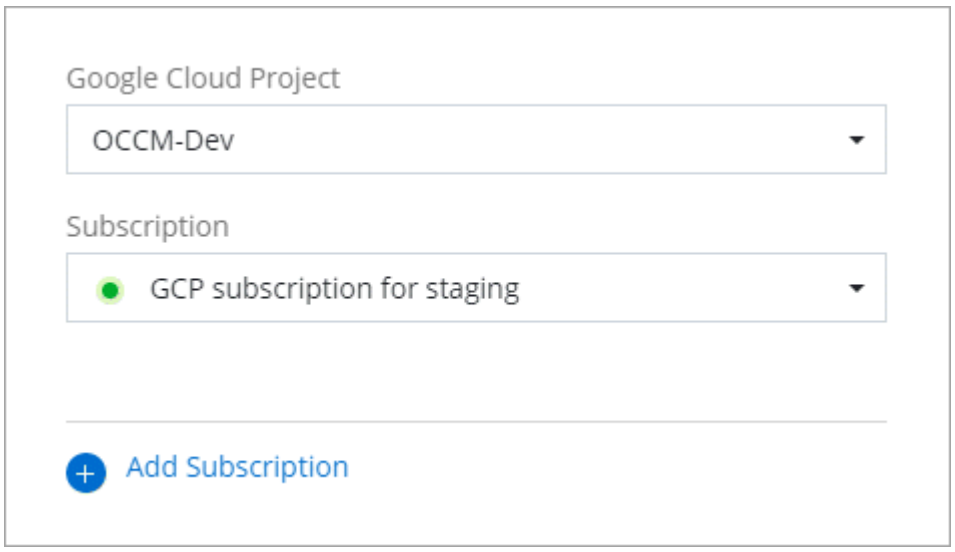
Google Cloud

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.
2. Seleccione el menú de acción para un conjunto de credenciales y luego seleccione **Suscripción asociada**.



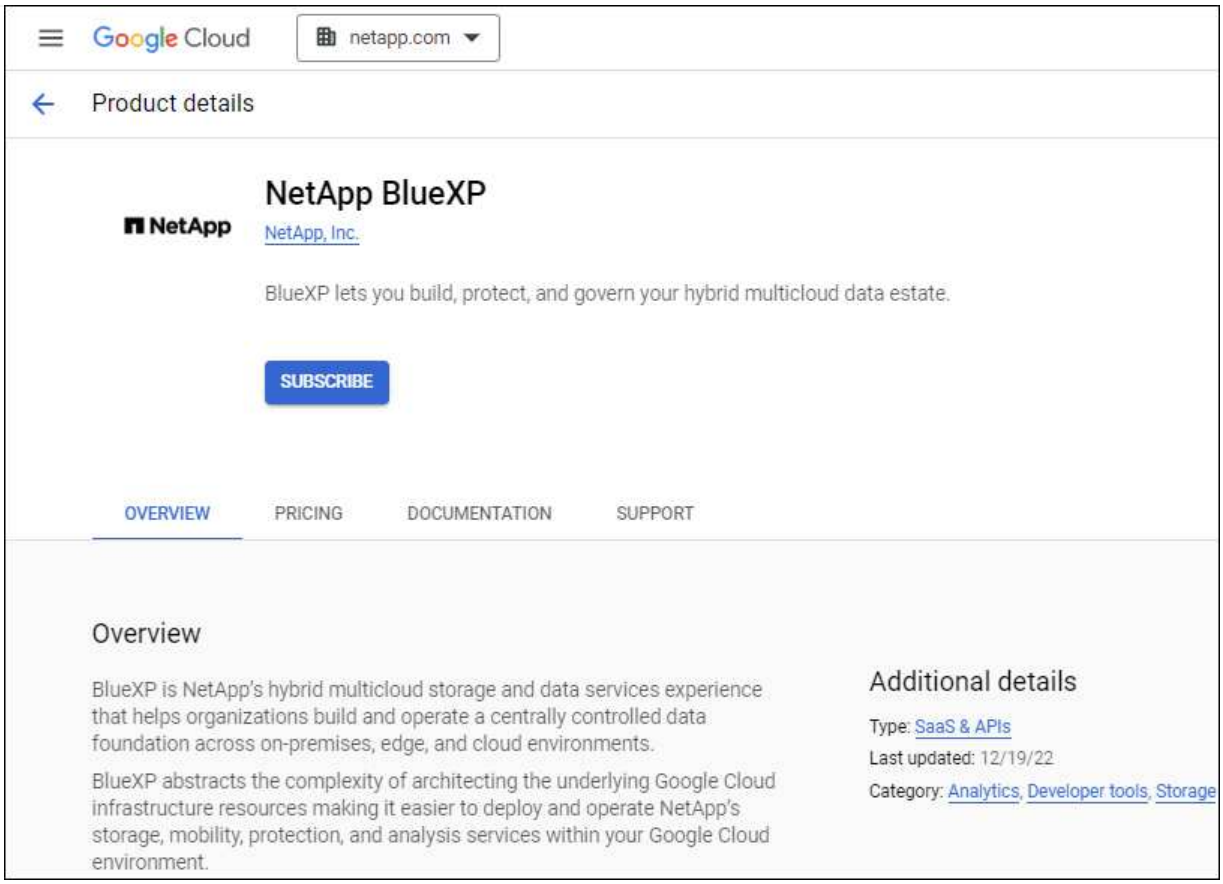
3. Para asociar las credenciales a una suscripción existente, seleccione un proyecto de Google Cloud y una suscripción en la lista desplegable y, a continuación, seleccione **asociado**.



4. Si aún no tiene una suscripción, seleccione **Agregar suscripción > continuar** y siga los pasos de Google Cloud Marketplace.

Antes de completar los siguientes pasos, asegúrese de que tiene privilegios de administrador de facturación en su cuenta de Google Cloud así como un inicio de sesión de BlueXP.

a. Cuando se le haya redirigido a. "Página de BlueXP de NetApp en Google Cloud Marketplace", asegúrese de seleccionar el proyecto correcto en el menú de navegación superior.

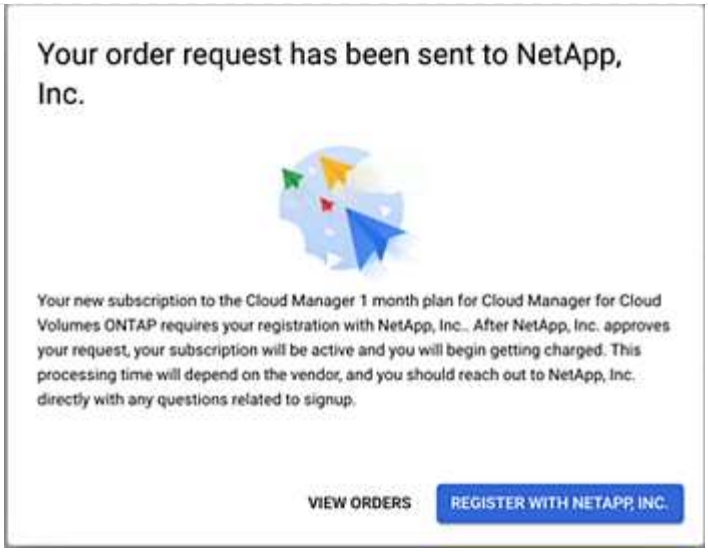


b. Seleccione **Suscribirse**.
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.
d. Seleccione **Suscribirse**.

   Este paso envía la solicitud de transferencia a NetApp.

e. En el cuadro de diálogo emergente, seleccione **Registro con NetApp, Inc.**

   Este paso debe completarse para vincular la suscripción a Google Cloud a su cuenta de BlueXP. El proceso de vinculación de una suscripción no está completo hasta que se le redirigirá de esta página y, a continuación, inicie sesión en BlueXP.



f. Siga los pasos de la página **asignación de suscripción**:

> Si alguien de su organización ya se ha suscrito a la suscripción de NetApp BlueXP desde su cuenta de facturación, se le redirigirá a "La página Cloud Volumes ONTAP en el sitio Web de BlueXP" en su lugar. Si esto no se realiza de forma inesperada, póngase en contacto con el equipo de ventas de NetApp. Google sólo activa una suscripción por cuenta de facturación de Google.

- Seleccione las cuentas de BlueXP con las que desea asociar esta suscripción.
- En el campo **sustituir suscripción existente**, elija si desea sustituir automáticamente la suscripción existente para una cuenta con esta nueva suscripción.

  BlueXP reemplaza la suscripción existente para todas las credenciales de la cuenta con esta nueva suscripción. Si alguna vez no se ha asociado un conjunto de credenciales a una suscripción, esta nueva suscripción no se asociará a dichas credenciales.

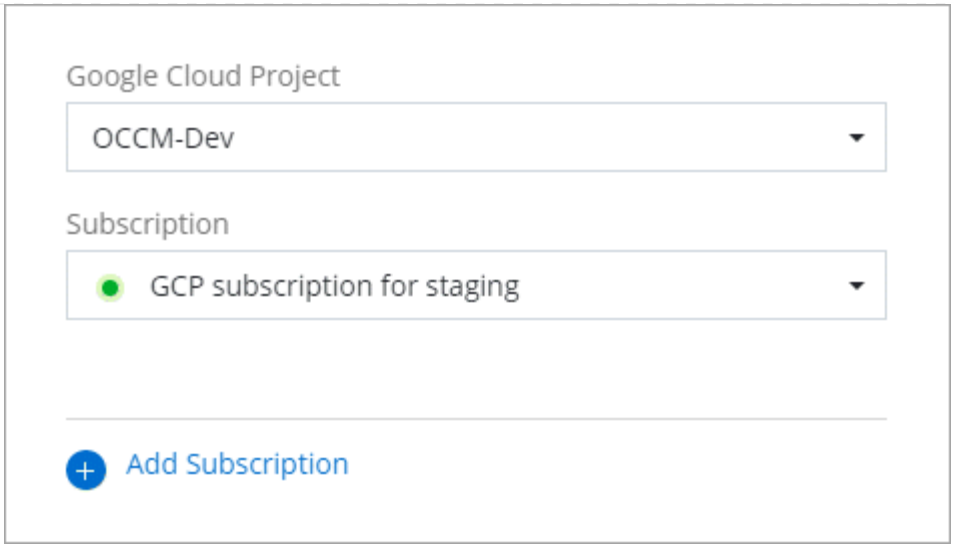
Para el resto de cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

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

Suscríbete a BlueXP desde Google Cloud Marketplace

a. Una vez completado este proceso, vuelva a la página credenciales de BlueXP y seleccione esta nueva suscripción.



Enlaces relacionados

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

Qué puede hacer después (modo restringido)

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

Para obtener ayuda, consulte la documentación de estos servicios:

- "Documentos de Amazon FSX para ONTAP"
- "Documentos de Azure NetApp Files"
- "Documentos de backup y recuperación"
- "Documentos de clasificación"
- "Documentos de Cloud Volumes ONTAP"
- "Documentos del clúster ONTAP en las instalaciones"
- "Documentos de replicación"

Enlace relacionado

"Modos de implementación de BlueXP"