



# **Configure un conector**

## **Set up and administration**

NetApp

March 13, 2023

# Tabla de Contenido

- Configure un conector ..... 1
  - Más información sobre conectores ..... 1
  - Cree un conector en AWS desde BlueXP ..... 5
  - Cree un conector en Azure desde BlueXP ..... 11
  - Crear un conector en Google Cloud desde BlueXP ..... 28
  - Cree un conector en una región gubernamental ..... 41

# Configure un conector

## Más información sobre conectores

En la mayoría de los casos, un administrador de cuentas de BlueXP necesitará poner en marcha un *Connector* en su red local o en la nube. El conector es un componente crucial para el uso diario de BlueXP. Permite a BlueXP gestionar los recursos y procesos de su entorno de cloud público.

### Cuando se necesita un conector

Se necesita un conector para las siguientes funciones y servicios de BlueXP:

- Funciones de gestión de Amazon FSX para ONTAP
- Detección de Amazon S3
- Descubrimiento de Azure Blob
- Backup en el cloud
- Cloud Data SENSE
- Organización en niveles del cloud
- Cloud Volumes ONTAP
- Sistemas E-Series
- Caché de archivos global
- Descubrimiento de Google Cloud Storage
- Clústeres de Kubernetes
- Integración de clústeres de ONTAP en las instalaciones con servicios de datos de BlueXP
- StorageGRID

Se requiere un conector **not** para los siguientes servicios:

- Asesor digital

En casi todos los casos, puede añadir una licencia al monedero digital sin conector.

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

- Creación de entornos de trabajo de Amazon FSX para ONTAP

Aunque no es necesario un conector para crear un entorno de trabajo, es necesario crear y gestionar volúmenes, replicar datos e integrar FSX para ONTAP con servicios de cloud de NetApp, como Data Sense y Cloud Sync.

- Azure NetApp Files

Aunque no es necesario un conector para configurar y gestionar Azure NetApp Files, se requiere un conector si desea utilizar Cloud Data Sense para analizar datos de Azure NetApp Files.

- Cloud Volumes Service para Google Cloud
- Cloud Sync
- Detección directa de clústeres de ONTAP en las instalaciones

Aunque no es necesario un conector para la detección directa de un clúster ONTAP en las instalaciones, se necesita un conector si desea aprovechar las características adicionales de BlueXP.

["Obtenga más información acerca de las opciones de detección y gestión para clústeres de ONTAP en las instalaciones"](#)

## Ubicaciones admitidas

Se admite un conector en las siguientes ubicaciones:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- En sus instalaciones
- En sus instalaciones, sin acceso a Internet

### Tenga nota sobre implementaciones de Azure

Si pone en marcha el conector en Azure, debe ponerse en marcha en la misma región de Azure que los sistemas de Cloud Volumes ONTAP que gestiona o en ["Par de regiones de Azure"](#) Para los sistemas Cloud Volumes ONTAP. Este requisito garantiza que se utilice una conexión de enlace privado de Azure entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas. ["Conozca cómo Cloud Volumes ONTAP utiliza un enlace privado de Azure"](#).

### Nota sobre implementaciones de Google Cloud

Si desea crear un sistema Cloud Volumes ONTAP en Google Cloud, debe tener un conector que también funcione en Google Cloud. No puede utilizar un conector que se ejecute en AWS, Azure o en las instalaciones.

## Los conectores deben permanecer en funcionamiento

Un conector debe permanecer en funcionamiento en todo momento. Es importante para la salud y el funcionamiento continuos de los servicios que usted habilita.

Por ejemplo, un conector es un componente clave en el estado y la operación de Cloud Volumes ONTAP. Si el conector está apagado, los sistemas PAYGO de Cloud Volumes ONTAP y los sistemas BYOL basados en capacidad se apagan después de perder la comunicación con un conector durante más de 14 días. Esto sucede porque el conector actualiza las licencias del sistema cada día.



Si su sistema Cloud Volumes ONTAP tiene una licencia BYOL basada en nodos, el sistema seguirá ejecutándose transcurridos 14 días porque la licencia se instala en el sistema Cloud Volumes ONTAP.

BlueXP le notificará si su conector ha sido apagado durante 14 días o más. ["Más información sobre las notificaciones de BlueXP"](#).

## Cómo crear un conector

Un administrador de cuentas de BlueXP puede crear un conector de varias maneras:

- Directamente de BlueXP (recomendado)
  - ["Cree en AWS"](#)
  - ["Cree en Azure"](#)
  - ["Crear en GCP"](#)
- Mediante la instalación manual del software en su propio host Linux
  - ["En un host que tiene acceso a Internet"](#)
  - ["En un host en una ubicación que no tiene acceso a Internet"](#)
- Desde el mercado de su proveedor de cloud
  - ["Mercado AWS"](#)
  - ["Azure Marketplace"](#)

Si trabaja en una región gubernamental, necesita implementar un conector desde el mercado de su proveedor de cloud o instalar manualmente el software del conector en un host Linux existente. No puede desplegar el conector en una región gubernamental desde el sitio web de BlueXP SaaS.

## Permisos

Se necesitan permisos específicos para crear el conector y se necesita otro conjunto de permisos para la propia instancia del conector.

### Permisos para crear un conector

El usuario que crea un conector a partir de BlueXP necesita permisos específicos para implementar la instancia en su proveedor de cloud de elección.

- ["Consulte los permisos de AWS necesarios"](#)
- ["Consulte los permisos de Azure necesarios"](#)
- ["Consulte los permisos necesarios de Google Cloud"](#)

### Permisos para la instancia de conector

El conector necesita permisos específicos de proveedor de cloud para realizar operaciones en su nombre. Por ejemplo, para poner en marcha y gestionar Cloud Volumes ONTAP.

Cuando crea un conector directamente desde BlueXP, BlueXP crea el conector con los permisos que necesita. No hay nada que usted necesita hacer.

Si crea el conector usted mismo desde AWS Marketplace, Azure Marketplace o mediante la instalación manual del software, tendrá que asegurarse de que cuenta con los permisos adecuados.

- ["Conozca cómo el conector utiliza los permisos de AWS"](#)
- ["Conozca cómo el conector utiliza los permisos de Azure"](#)
- ["Descubra cómo el conector utiliza los permisos de Google Cloud"](#)

## Actualizaciones de conectores

Normalmente actualizamos el software del conector cada mes para introducir nuevas funciones y para proporcionar mejoras de estabilidad. Aunque la mayoría de los servicios y características de la plataforma BlueXP se ofrecen a través de software basado en SaaS, algunas características y funciones dependen de la versión del conector. Que incluye gestión de Cloud Volumes ONTAP, gestión de clústeres ONTAP en las instalaciones, configuración y ayuda.

El conector actualiza automáticamente su software a la última versión, siempre que tenga acceso saliente a Internet para obtener la actualización de software.

## Número de entornos de trabajo por conector

Un conector puede gestionar varios entornos de trabajo en BlueXP. El número máximo de entornos de trabajo que debe gestionar un único conector varía. Depende del tipo de entorno laboral, del número de volúmenes, de la cantidad de capacidad que se administra y del número de usuarios.

Si tiene una puesta en marcha a gran escala, trabaje con su representante de NetApp para dimensionar el entorno. Si experimenta algún problema a lo largo del camino, póngase en contacto con nosotros a través del chat en el producto.

## Cuándo usar varios conectores

En algunos casos, es posible que sólo necesite un conector, pero es posible que necesite dos o más conectores.

A continuación, se muestran algunos ejemplos:

- Utiliza un entorno multicloud (AWS y Azure), por lo que tiene un conector en AWS y otro en Azure. Cada una de ellas gestiona los sistemas Cloud Volumes ONTAP que se ejecutan en estos entornos.
- Un proveedor de servicios puede utilizar una cuenta de NetApp para proporcionar servicios a sus clientes mientras utiliza otra cuenta para proporcionar recuperación ante desastres para una de sus unidades de negocio. Cada cuenta tendría conectores independientes.

## Uso de varios conectores con el mismo entorno de trabajo

Puede gestionar un entorno de trabajo con varios conectores al mismo tiempo para fines de recuperación ante desastres. Si se cae un conector, puede cambiar al otro conector para gestionar inmediatamente el entorno de trabajo.

Para configurar esta configuración:

1. "[Cambie a otro conector](#)"
2. Detectar el entorno de trabajo existente.
  - "[Agregue sistemas Cloud Volumes ONTAP existentes a BlueXP](#)"
  - "[Detectar clústeres de ONTAP](#)"
3. Ajuste la "[Modo de gestión de la capacidad](#)"

Sólo el conector principal debe ajustarse en **modo automático**. Si cambia a otro conector para fines de DR, puede cambiar el modo de gestión de capacidad según sea necesario.

## Cuándo cambiar entre conectores

Al crear el primer conector, BlueXP utiliza automáticamente ese conector para cada entorno de trabajo adicional que cree. Una vez creado un conector adicional, deberá cambiar entre ellos para ver los entornos de trabajo específicos de cada conector.

["Aprenda a cambiar entre conectores"](#).

## La interfaz de usuario local

Mientras debe realizar casi todas las tareas de la ["Interfaz de usuario de SaaS"](#), una interfaz de usuario local todavía está disponible en el conector. Esta interfaz es necesaria si instala el conector en un entorno que no tiene acceso a Internet (como una región gubernamental) y para algunas tareas que se deben realizar desde el propio conector, en lugar de la interfaz SaaS:

- ["Establecimiento de un servidor proxy"](#)
- Instalación de un parche (Normalmente, trabajará con el personal de NetApp para instalar un parche).
- Descargando mensajes de AutoSupport (Normalmente dirigido por el personal de NetApp cuando tiene problemas)

["Aprenda a acceder a la interfaz de usuario local"](#).

## Cree un conector en AWS desde BlueXP

Un administrador de cuentas de BlueXP necesita implementar un *Connector* antes de poder utilizar la mayoría de las funciones de BlueXP. Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público.

Estos pasos describen cómo crear un conector en una región comercial de AWS directamente desde el sitio web de BlueXP SaaS.

- ["Aprenda a desplegar un conector en una región gubernamental"](#)
- ["Obtenga información sobre otras formas de desplegar un conector"](#)

## Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1

### Configure la autenticación

Para iniciar Connector en AWS, BlueXP debe autenticarse con AWS asumiendo un rol IAM o utilizando claves de acceso de AWS. Con cualquiera de las dos opciones, se requiere una política de IAM.

[Ver el rol IAM](#) o [siga las instrucciones paso a paso](#).

2

### Configure las redes

Se necesita un VPC y una subred con acceso de salida a Internet hacia extremos específicos. Si se requiere un servidor proxy para Internet de salida, necesitará la dirección IP, las credenciales y el certificado HTTPS.

[Ver los requisitos de red.](#)

3

### Cree el conector

Haga clic en el menú desplegable conector, seleccione **Agregar conector** y siga las indicaciones.

[Siga las instrucciones paso a paso.](#)

## Configure la autenticación de AWS

BlueXP debe autenticarse con AWS para poder implementar la instancia de Connector en su VPC. Es posible elegir uno de los siguientes métodos de autenticación:

- Deje que BlueXP asuma una función de IAM que tenga los permisos necesarios
- Proporcione una clave secreta y de acceso de AWS para un usuario IAM que tenga los permisos necesarios

Con cualquiera de las dos opciones, primero debe empezar creando una política de IAM que incluya los permisos necesarios.

### Cree una política de IAM

Esta directiva sólo contiene los permisos necesarios para iniciar la instancia de Connector en AWS desde BlueXP. No utilice esta política para otras situaciones.

Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos a la instancia de Connector que permite al conector administrar los recursos de su entorno de nube pública.

### Pasos

1. Vaya a la consola IAM de AWS.
2. Haga clic en **Directivas > Crear directiva**.
3. Haga clic en **JSON**.
4. Copie y pegue la siguiente política:

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam:PutRolePolicy",
      "iam:CreateInstanceProfile",
      "iam>DeleteRolePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:PassRole",
    ]
  }]
}
```



```

        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    }
}

```

```

    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. Haga clic en **Siguiente** y agregue etiquetas, si es necesario.
6. Haga clic en **Siguiente** e introduzca un nombre y una descripción.
7. Haga clic en **Crear directiva**.

### El futuro

Adjunte la política a una función de IAM que BlueXP puede asumir o a un usuario de IAM.

### Configurar un rol de IAM

Configurar una función de IAM que BlueXP puede asumir para implementar Connector en AWS.

#### Pasos

1. Vaya a la consola AWS IAM de la cuenta de destino.
2. En Access Management, haga clic en **roles > Crear función** y siga los pasos para crear la función.

No olvide hacer lo siguiente:

- En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
  - Seleccione **otra cuenta de AWS** e introduzca el ID de la cuenta de BlueXP SaaS: 952013314444
  - Seleccione la directiva que ha creado en la sección anterior.
3. Después de crear la función, copie la función ARN para que pueda pegarla en BlueXP al crear el conector.

### Resultado

El rol IAM ahora tiene los permisos necesarios.

### Configurar permisos para un usuario de IAM

Al crear un conector, puede proporcionar una clave secreta y de acceso a AWS para un usuario IAM con los permisos necesarios para implementar la instancia del conector.

#### Pasos

1. En la consola AWS IAM, haga clic en **usuarios** y, a continuación, seleccione el nombre de usuario.
2. Haga clic en **Agregar permisos > Adjuntar directivas existentes directamente**.
3. Seleccione la política que ha creado.
4. Haga clic en **Siguiente** y, a continuación, en **Agregar permisos**.
5. Asegúrese de tener acceso a una clave de acceso y a una clave secreta para el usuario de IAM.

### Resultado

Ahora el usuario de AWS tiene los permisos necesarios para crear el conector desde BlueXP. Deberá

especificar las claves de acceso de AWS para este usuario cuando se le solicite BlueXP.

## Configure las redes

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.


### Conexión a redes de destino

Un conector requiere una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que tiene previsto habilitar.

Por ejemplo, si instala un conector en su red corporativa, debe configurar una conexión VPN a la red virtual en la que inicie Cloud Volumes ONTAP.

### Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): <ul style="list-style-type: none"><li>• Formación CloudFormation</li><li>• Cloud computing elástico (EC2)</li><li>• Servicio de gestión de claves (KMS)</li><li>• Servicio de token de seguridad (STS)</li><li>• Simple Storage Service (S3)</li></ul>	Para gestionar recursos en AWS. El extremo exacto depende de la región en la que se despliega el conector. <a href="#">"Consulte la documentación de AWS para obtener más detalles"</a>
https://support.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	<div> El conector se está comunicando actualmente con "cloudmanager.cloud.netapp.com" pero empezará a ponerse en contacto con "api.bluexp.netapp.com" en una próxima versión.</div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Para actualizar el conector y sus componentes de Docker.

### Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico saliente de Internet, obtenga la siguiente información acerca del proxy HTTP o HTTPS:

- Dirección IP
- Credenciales
- Certificado HTTPS

## Grupo de seguridad

No hay tráfico entrante en el conector, a menos que lo inicie o si el conector se utiliza como proxy para los mensajes AutoSupport. HTTP y HTTPS proporcionan acceso al ["Interfaz de usuario local"](#), que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

## Limitación de dirección IP

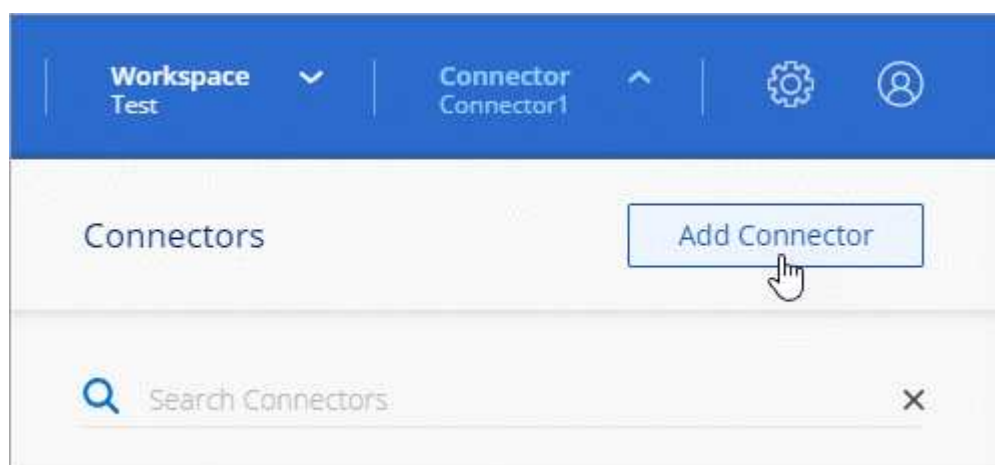
Puede haber un conflicto con las direcciones IP en el rango 172. ["Obtenga más información sobre esta limitación"](#).

## Cree un conector

BlueXP permite crear un conector en AWS directamente desde su interfaz de usuario.

### Pasos

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Elija **Amazon Web Services** como su proveedor de cloud y haga clic en **continuar**.
3. En la página **despliegue de un conector**, revise los detalles sobre lo que necesitará. Dispone de dos opciones:
  - a. Haga clic en **continuar** para preparar la implementación utilizando la guía del producto. Cada paso de la guía del producto incluye la información que se incluye en esta página de la documentación.
  - b. Haga clic en **Ir a implementación** si ya ha preparado siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el conector:
  - **Prepárese:** Revise lo que necesitará.
  - **Credenciales de AWS:** Especifique su región de AWS y, a continuación, elija un método de autenticación, que es una función de IAM que BlueXP puede asumir o una clave de acceso y clave secreta de AWS.



Si elige **asumir función**, puede crear el primer conjunto de credenciales desde el asistente de implementación del conector. Debe crear cualquier conjunto adicional de credenciales desde la página Credentials. A continuación, estarán disponibles en el asistente en una lista desplegable. ["Aprenda a añadir credenciales adicionales"](#).

- **Detalles:** Proporcione detalles sobre el conector.
  - Escriba un nombre para la instancia.
  - Añada etiquetas personalizadas (metadatos) a la instancia.
  - Elija si desea que BlueXP cree una nueva función que tenga los permisos necesarios o si desea seleccionar una función existente con la que haya configurado ["los permisos necesarios"](#).
  - Elija si desea cifrar los discos EBS del conector. Tiene la opción de utilizar la clave de cifrado predeterminada o utilizar una clave personalizada.
- **Red:** Especifique un VPC, una subred y un par de claves para la instancia, elija si desea habilitar una dirección IP pública y, opcionalmente, especifique una configuración de proxy (se admiten HTTP y HTTPS).

Asegúrese de que tiene el par de llaves correcto para usar con el conector. Sin un par de teclas, no podrá acceder a la máquina virtual conector.
- **Grupo de seguridad:** Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.
- **Revisión:** Revise sus selecciones para verificar que su configuración es correcta.

#### 5. Haga clic en **Agregar**.

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

#### Después de terminar

Si tiene cubos Amazon S3 en la misma cuenta AWS en la que creó el conector, verá que aparecerá un entorno de trabajo Amazon S3 en el lienzo automáticamente. ["Obtenga más información sobre lo que puede hacer con este entorno de trabajo"](#).

## Abra el puerto 3128 para los mensajes de AutoSupport

Si tiene previsto implementar sistemas Cloud Volumes ONTAP en una subred en la que no esté disponible una conexión a Internet saliente, BlueXP configura automáticamente Cloud Volumes ONTAP para que utilice el conector como servidor proxy.

El único requisito es asegurarse de que el grupo de seguridad del conector permita conexiones *entrante* a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Si utiliza el grupo de seguridad predeterminado para Cloud Volumes ONTAP, no es necesario realizar cambios en su grupo de seguridad. Pero si tiene pensado definir reglas de salida estrictas para Cloud Volumes ONTAP, también tendrá que asegurarse de que el grupo de seguridad Cloud Volumes ONTAP permita conexiones *saliente* a través del puerto 3128.

## Cree un conector en Azure desde BlueXP

Un administrador de cuentas de BlueXP necesita implementar un *Connector* antes de

poder utilizar la mayoría de las funciones de BlueXP. Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público.

Estos pasos describen cómo crear un conector en una región comercial de Azure directamente desde el sitio web de SaaS de BlueXP.

- ["Aprenda a desplegar un conector en una región gubernamental"](#)
- ["Obtenga información sobre otras formas de desplegar un conector"](#)

## Descripción general

Para implementar un conector, debe proporcionar a BlueXP un inicio de sesión que tenga los permisos necesarios para crear el conector VM en Azure.

Dispone de dos opciones:

1. Inicie sesión con su cuenta de Microsoft cuando se le solicite. Esta cuenta debe tener permisos de Azure específicos. Esta es la opción predeterminada.

[Siga los pasos que aparecen a continuación para comenzar.](#)

2. Proporcionar detalles acerca de un director de servicio de Azure AD. Este principal de servicio también requiere permisos específicos.

[Siga los pasos que aparecen a continuación para comenzar.](#)

## Nota sobre las regiones de Azure

El conector debe ponerse en marcha en la misma región de Azure que los sistemas Cloud Volumes ONTAP que gestione o en ["Par de regiones de Azure"](#) Para los sistemas Cloud Volumes ONTAP. Este requisito garantiza que se utilice una conexión de enlace privado de Azure entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas.

["Conozca cómo Cloud Volumes ONTAP utiliza un enlace privado de Azure"](#)

## Configure las redes

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.


### Conexión a redes de destino

Un conector requiere una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que tiene previsto habilitar.

Por ejemplo, si instala un conector en su red corporativa, debe configurar una conexión VPN a la red virtual en la que inicie Cloud Volumes ONTAP.

### Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> <a href="https://core.windows.net">https://core.windows.net</a>	Para gestionar recursos en regiones públicas de Azure.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.us">https://login.microsoftonline.us</a> <a href="https://blob.core.usgovcloudapi.net">https://blob.core.usgovcloudapi.net</a> <a href="https://core.usgovcloudapi.net">https://core.usgovcloudapi.net</a>	Para gestionar recursos en regiones gubernamentales de Azure.
<a href="https://management.azure.microsoft.scloud">https://management.azure.microsoft.scloud</a> <a href="https://login.microsoftonline.microsoft.scloud">https://login.microsoftonline.microsoft.scloud</a> <a href="https://blob.core.microsoft.scloud">https://blob.core.microsoft.scloud</a> <a href="https://core.microsoft.scloud">https://core.microsoft.scloud</a>	Para administrar recursos en la región de Azure IL6.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	Para gestionar recursos en regiones de Azure China.
<a href="https://support.netapp.com">https://support.netapp.com</a>	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
<a href="https://*.api.blueexp.netapp.com">https://*.api.blueexp.netapp.com</a> <a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	<div>  <p>El conector se está comunicando actualmente con "cloudmanager.cloud.netapp.com" pero empezará a ponerse en contacto con "api.blueexp.netapp.com" en una próxima versión.</p> </div>
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	Para actualizar el conector y sus componentes de Docker.

## Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico saliente de Internet, obtenga la siguiente información acerca del proxy HTTP o HTTPS:

- Dirección IP
- Credenciales
- Certificado HTTPS

## Grupo de seguridad

No hay tráfico entrante en el conector, a menos que lo inicie o si el conector se utiliza como proxy para los mensajes AutoSupport. HTTP y HTTPS proporcionan acceso al ["Interfaz de usuario local"](#), que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

## Limitación de dirección IP

Puede haber un conflicto con las direcciones IP en el rango 172. ["Obtenga más información sobre esta limitación"](#).

## Cree un conector con su cuenta de Azure

La forma predeterminada de crear un conector en Azure es iniciar sesión con su cuenta de Azure cuando se le solicite. El formulario de inicio de sesión es propiedad de Microsoft y está alojado en él. Sus credenciales no se proporcionan a NetApp.

### Configure permisos para la cuenta de Azure

Antes de implementar un conector desde BlueXP, debe asegurarse de que su cuenta de Azure tenga los permisos correctos.

#### Pasos

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



Esta política solo contiene los permisos necesarios para iniciar Connector VM en Azure desde BlueXP. No utilice esta política para otras situaciones. Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos al conector VM que permite al conector administrar los recursos de su entorno de nube pública.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
```



```

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
],

```

```

    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
  }
}

```

2. Modifique el JSON añadiendo su ID de suscripción de Azure al ámbito asignable.

#### ejemplo

```

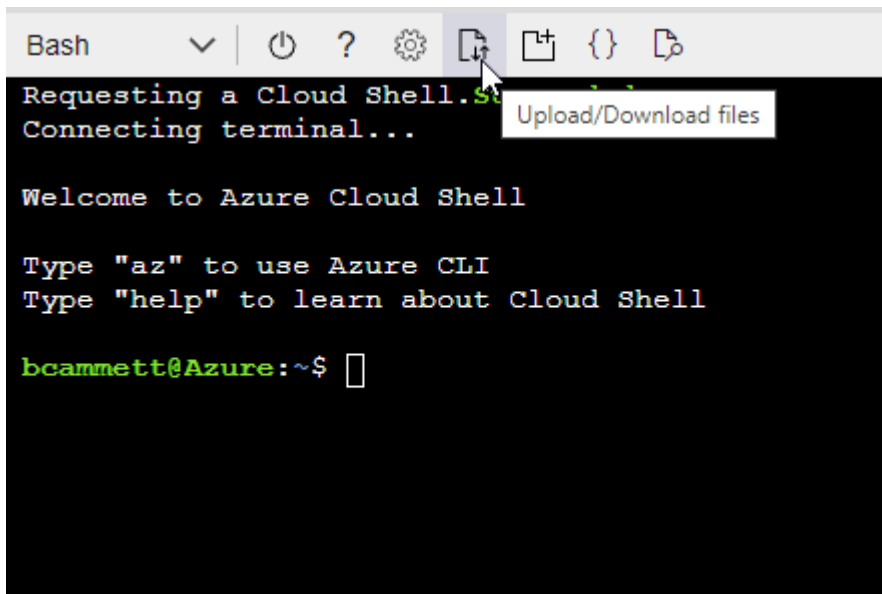
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

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

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

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



- c. Introduzca el siguiente comando CLI de Azure:

```

az role definition create --role-definition
Policy_for_Setup_As_Service_Azure.json

```

Ahora debería tener una función personalizada denominada *Azure SetupAsService*.

4. Asigne la función al usuario que implementará Connector desde BlueXP:

- a. Abra el servicio **Suscripciones** y seleccione la suscripción del usuario.
- b. Haga clic en **Control de acceso (IAM)**.
- c. Haga clic en **Agregar > Agregar asignación de rol** y, a continuación, agregue los permisos:
  - Seleccione el rol **Azure SetupAsService** y haga clic en **Siguiente**.



Azure SetupAsService es el nombre predeterminado proporcionado en la política de implementación de Connector para Azure. Si seleccionó otro nombre para el rol, seleccione ese nombre.

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

## Resultado

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

## Cree el conector iniciando sesión con su cuenta de Azure

BlueXP permite crear un conector en Azure directamente desde su interfaz de usuario.

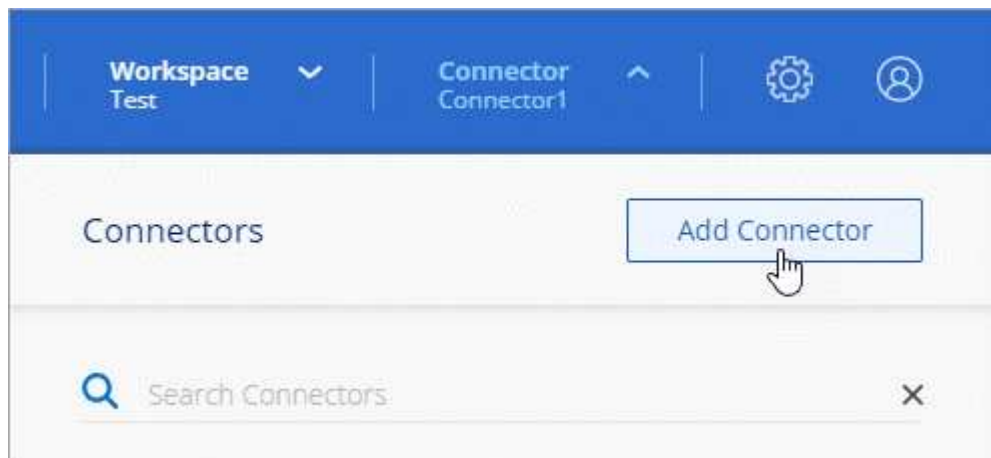
### Lo que necesitará

- Una suscripción a Azure.
- Una red virtual y una subred en su región de Azure preferida.
- Si no quiere que BlueXP cree automáticamente una función de Azure para Connector, tendrá que crear la suya propia ["uso de la política en esta página"](#).

Estos permisos son para la propia instancia de Connector. Se trata de un conjunto de permisos diferente al que se configuró anteriormente para desplegar el conector.

## Pasos

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Elija **Microsoft Azure** como proveedor de cloud.
3. En la página **despliegue de un conector**, revise los detalles sobre lo que necesitará. Dispone de dos opciones:
  - a. Haga clic en **continuar** para preparar la implementación utilizando la guía del producto. Cada paso incluye información contenida en esta página de la documentación.
  - b. Haga clic en **Ir a implementación** si ya ha preparado siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el conector:

- Si se le solicita, inicie sesión en su cuenta de Microsoft, que debería tener los permisos necesarios para crear la máquina virtual.

El formulario es propiedad de Microsoft y está alojado en él. Sus credenciales no se proporcionan a NetApp.



Si ya ha iniciado sesión en una cuenta de Azure, BlueXP utilizará esa cuenta automáticamente. Si tiene varias cuentas, es posible que deba cerrar la sesión primero para asegurarse de utilizar la cuenta correcta.

- **Autenticación de VM:** Elija una suscripción de Azure, una ubicación, un nuevo grupo de recursos o un grupo de recursos existente y, a continuación, elija un método de autenticación.
- **Detalles:** Escriba un nombre para la instancia, especifique etiquetas y elija si desea que BlueXP cree una nueva función que tenga los permisos necesarios o si desea seleccionar una función existente con la que se haya configurado "[los permisos necesarios](#)".

Tenga en cuenta que puede elegir las suscripciones asociadas a esta función. Cada suscripción que elija proporciona al conector permisos para implementar Cloud Volumes ONTAP en esas suscripciones.

- **Red:** Elija un vnet y una subred, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
- **Grupo de seguridad:** Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.
- **Revisión:** Revise sus selecciones para verificar que su configuración es correcta.

5. Haga clic en **Agregar**.

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

### Después de terminar

Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP. Si sólo tiene Administradores de cuentas, no es necesario asociar el conector a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todas las áreas de trabajo de BlueXP de forma predeterminada. "[Leer más](#)".

Si dispone de almacenamiento de Azure Blob en la misma cuenta de Azure en la que creó el conector, verá que aparece un entorno de trabajo de Azure Blob en el lienzo automáticamente. "[Obtenga más información sobre lo que puede hacer con este entorno de trabajo](#)".

## Cree un conector con un director de servicio

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

### Concesión de permisos de Azure con un director de servicio

Conceda los permisos necesarios para implementar un conector en Azure mediante la creación y configuración de un servicio principal en Azure Active Directory y la obtención de las credenciales de Azure que BlueXP necesita.

#### Pasos

1. [Cree una aplicación de Azure Active Directory](#).
2. [Asigne la aplicación a una función](#).
3. [Añada permisos de API de administración de servicios de Windows Azure](#).
4. [Obtener el ID de aplicación y el ID de directorio](#).
5. [Cree un secreto de cliente](#).

#### Cree una aplicación de Azure Active Directory

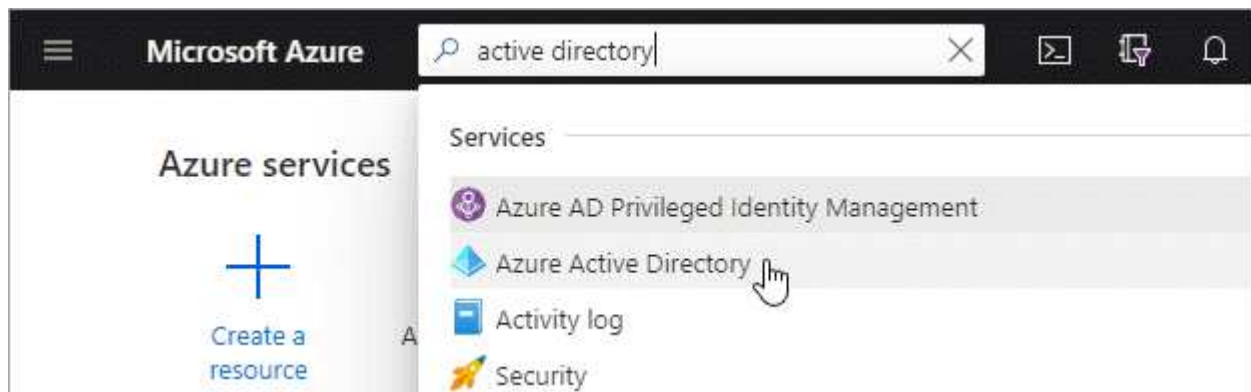
Cree una aplicación de Azure Active Directory (AD) y una entidad de servicio que BlueXP pueda utilizar para implementar Connector.

#### Antes de empezar

Debe tener los permisos adecuados en Azure para crear una aplicación de Active Directory y asignar la aplicación a un rol. Para obtener más información, consulte ["Documentación de Microsoft Azure: Permisos necesarios"](#).

#### Pasos

1. Desde el portal de Azure, abra el servicio **Azure Active Directory**.



2. En el menú, haga clic en **App registrars**.
3. Haga clic en **Nuevo registro**.
4. 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.

5. Haga clic en **Registrar**.

## Resultado

Ha creado la aplicación AD y el director de servicio.

## Asigne la aplicación a una función

Debe enlazar la entidad de servicio a la suscripción a Azure en la que planea implementar el conector y asignarle el rol personalizado "Azure SetupAsService".

## Pasos

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



Esta política solo contiene los permisos necesarios para iniciar Connector VM en Azure desde BlueXP. No utilice esta política para otras situaciones. Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos al conector VM que permite al conector administrar los recursos de su entorno de nube pública.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
```

```

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
  "Microsoft.Network/virtualNetworks/virtualMachines/read",
  "Microsoft.Network/publicIPAddresses/write",
  "Microsoft.Network/publicIPAddresses/read",
  "Microsoft.Network/publicIPAddresses/delete",
  "Microsoft.Network/networkSecurityGroups/securityRules/read",
  "Microsoft.Network/networkSecurityGroups/securityRules/write",
  "Microsoft.Network/networkSecurityGroups/securityRules/delete",
  "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
  "Microsoft.Network/networkInterfaces/ipConfigurations/read",
  "Microsoft.Resources/deployments/operations/read",
  "Microsoft.Resources/deployments/read",
  "Microsoft.Resources/deployments/delete",
  "Microsoft.Resources/deployments/cancel/action",
  "Microsoft.Resources/deployments/validate/action",
  "Microsoft.Resources/resources/read",
  "Microsoft.Resources/subscriptions/operationresults/read",
  "Microsoft.Resources/subscriptions/resourceGroups/delete",
  "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
  "Microsoft.Resources/subscriptions/resourceGroups/write",
  "Microsoft.Authorization/roleDefinitions/write",
  "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
  "Microsoft.Network/networkSecurityGroups/delete",
  "Microsoft.Storage/storageAccounts/delete",
  "Microsoft.Storage/storageAccounts/write",
  "Microsoft.Resources/deployments/write",
  "Microsoft.Resources/deployments/operationStatuses/read",
  "Microsoft.Authorization/roleAssignments/read"
],
"NotActions": [],
"AssignableScopes": [],
"Description": "Azure SetupAsService",
"IsCustom": "true"
}

```

2. Modifique el archivo JSON añadiendo su ID de suscripción de Azure al ámbito asignable.

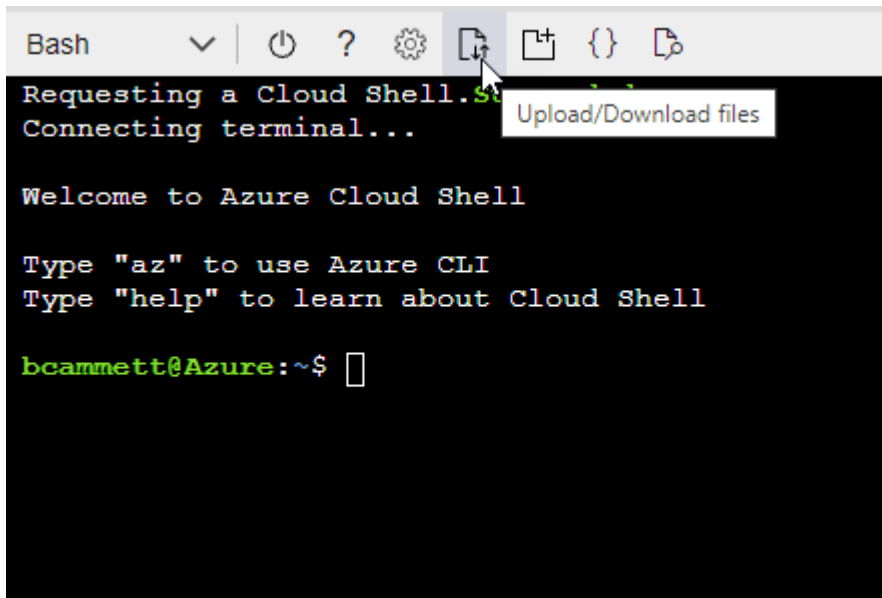
#### ejemplo

```
"AssignableScopes": [  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

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

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

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



- c. Introduzca el siguiente comando CLI de Azure:

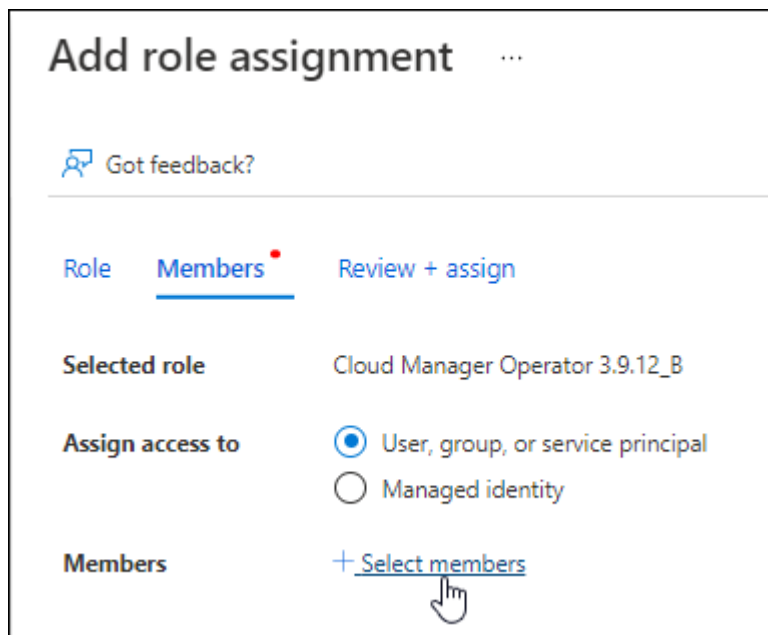
```
az role definition create --role-definition  
Policy_for_Setup_As_Service_Azure.json
```

Ahora debería tener una función personalizada denominada *Azure SetupAsService*.

4. Asigne la aplicación al rol:
  - a. En el portal de Azure, abra el servicio **Suscripciones**.
  - b. Seleccione la suscripción.
  - c. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
  - d. En la ficha **rol**, seleccione el rol **Azure SetupAsService** y haga clic en **Siguiente**.
  - e. En la ficha **Miembros**, realice los siguientes pasos:
    - Mantener seleccionado **Usuario, grupo o principal de servicio**.

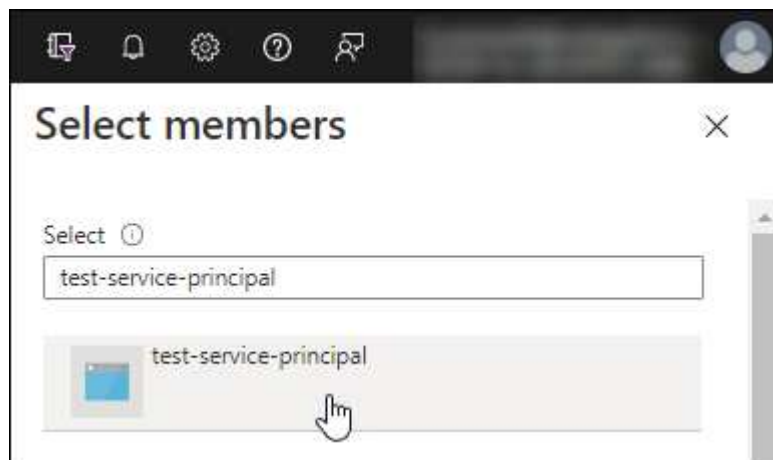


- Haga clic en **Seleccionar miembros**.



- Busque el nombre de la aplicación.

Veamos un ejemplo:



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

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

#### Añada permisos de API de administración de servicios de Windows Azure

El principal de servicio debe tener permisos de "API de administración de servicios de Windows Azure".

#### Pasos

1. En el servicio **Azure Active Directory**, haga clic en **App registrs** y seleccione la aplicación.
2. Haga clic en **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. Haga clic en **Access Azure Service Management como usuarios de la organización** y, a continuación, haga clic en **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
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

### Obtener el ID de aplicación y el ID de directorio

Al crear el conector desde BlueXP, debe proporcionar el ID de aplicación (cliente) y el ID de directorio (arrendatario) para la aplicación. BlueXP utiliza los identificadores para iniciar sesión mediante programación.

#### Pasos

1. En el servicio **Azure Active Directory**, haga clic en **App registrs** y seleccione la aplicación.
2. Copie el **ID de aplicación (cliente)** y el **ID de directorio (inquilino)**.



### Cree un secreto de cliente

Necesita crear un secreto de cliente y, a continuación, proporcionar BlueXP con el valor del secreto para que BlueXP pueda utilizarlo para autenticar con Azure AD.

#### Pasos

1. Abra el servicio **Azure Active Directory**.
2. Haga clic en **App registres** y seleccione su aplicación.
3. Haga clic en **certificados y secretos > Nuevo secreto de cliente**.

- Proporcione una descripción del secreto y una duración.
- Haga clic en **Agregar**.
- 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.

<a href="#">+ New client secret</a>		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

### Resultado

Su principal de servicio ahora está configurado y debe haber copiado el ID de aplicación (cliente), el ID de directorio (arrendatario) y el valor del secreto de cliente. Debe introducir esta información en BlueXP cuando cree el conector.

### Cree el conector iniciando sesión con el principal de servicio

BlueXP permite crear un conector en Azure directamente desde su interfaz de usuario.

#### Lo que necesitará

- Una suscripción a Azure.
- Una red virtual y una subred en su región de Azure preferida.
- Detalles sobre un servidor proxy, si su empresa requiere un proxy para todo el tráfico saliente de Internet:
  - Dirección IP
  - Credenciales
  - Certificado HTTPS
- Si no quiere que BlueXP cree automáticamente una función de Azure para Connector, tendrá que crear la suya propia ["uso de la política en esta página"](#).

Estos permisos son para la propia instancia de Connector. Se trata de un conjunto de permisos diferente al que se configuró anteriormente para desplegar el conector.

### Pasos

- Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Elija **Microsoft Azure** como proveedor de cloud.
3. En la página **despliegue de un conector**:
  - a. En **autenticación**, haga clic en **principal de servicio de Active Directory** e introduzca información acerca del principal de servicio de Azure Active Directory que concede los permisos necesarios:
    - ID de aplicación (cliente): Consulte [Obtener el ID de aplicación y el ID de directorio](#).
    - ID de directorio (arrendatario): Consulte [Obtener el ID de aplicación y el ID de directorio](#).
    - Client Secret: Consulte [Cree un secreto de cliente](#).
  - b. Haga clic en **Iniciar sesión**.
  - c. Ahora tiene dos opciones:
    - Haga clic en **continuar** para preparar la implementación utilizando la guía del producto. Cada paso de la guía del producto incluye la información que se incluye en esta página de la documentación.
    - Haga clic en **Ir a implementación** si ya ha preparado siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el conector:
  - **Autenticación de VM**: Elija una suscripción de Azure, una ubicación, un nuevo grupo de recursos o un grupo de recursos existente y, a continuación, elija un método de autenticación.
  - **Detalles**: Escriba un nombre para la instancia, especifique etiquetas y elija si desea que BlueXP cree una nueva función que tenga los permisos necesarios o si desea seleccionar una función existente con la que se haya configurado "[los permisos necesarios](#)".

Tenga en cuenta que puede elegir las suscripciones asociadas a esta función. Cada suscripción que elija proporciona al conector permisos para implementar Cloud Volumes ONTAP en esas suscripciones.
  - **Red**: Elija un vnet y una subred, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
  - **Grupo de seguridad**: Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.
  - **Revisión**: Revise sus selecciones para verificar que su configuración es correcta.
5. Haga clic en **Agregar**.

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

## Después de terminar

Debe asociar un conector a áreas de trabajo para que los administradores del área de trabajo puedan utilizar estos conectores para crear sistemas Cloud Volumes ONTAP. Si sólo tiene Administradores de cuentas, no es necesario asociar el conector a áreas de trabajo. Los administradores de cuentas tienen la posibilidad de acceder a todas las áreas de trabajo de BlueXP de forma predeterminada. ["Leer más"](#).

Si dispone de almacenamiento de Azure Blob en la misma cuenta de Azure en la que creó el conector, verá que aparece un entorno de trabajo de Azure Blob en el lienzo automáticamente. ["Obtenga más información sobre lo que puede hacer con este entorno de trabajo"](#).

## Abra el puerto 3128 para los mensajes de AutoSupport

Si tiene previsto implementar sistemas Cloud Volumes ONTAP en una subred en la que no esté disponible una conexión a Internet saliente, BlueXP configura automáticamente Cloud Volumes ONTAP para que utilice el conector como servidor proxy.

El único requisito es asegurarse de que el grupo de seguridad del conector permita conexiones *entrante* a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Si utiliza el grupo de seguridad predeterminado para Cloud Volumes ONTAP, no es necesario realizar cambios en su grupo de seguridad. Pero si tiene pensado definir reglas de salida estrictas para Cloud Volumes ONTAP, también tendrá que asegurarse de que el grupo de seguridad Cloud Volumes ONTAP permita conexiones *saliente* a través del puerto 3128.

## Crear un conector en Google Cloud desde BlueXP

Un administrador de cuentas de BlueXP necesita implementar un *Connector* antes de poder utilizar la mayoría de las funciones de BlueXP. ["Aprender cuando se necesita un conector"](#). Connector permite que BlueXP gestione recursos y procesos dentro de su entorno de cloud público.

Esta página describe cómo crear un conector en Google Cloud directamente desde BlueXP. ["Obtenga información sobre otras formas de desplegar un conector"](#).

Estos pasos deben ser completados por un usuario que tenga la función de administrador de cuentas. Un administrador de área de trabajo no puede crear un conector.



Al crear su primer entorno de trabajo de Cloud Volumes ONTAP, BlueXP le solicitará que cree un conector si aún no lo tiene.

## Inicio rápido

Empiece rápidamente siguiendo estos pasos o desplácese hacia abajo hasta las secciones restantes para obtener todos los detalles.

1

### Configure los permisos

- Asegúrese de que su cuenta de Google Cloud tiene los permisos correctos creando y adjuntando una función personalizada.

[Configure los permisos para desplegar el conector.](#)

- Al crear el conector VM, debe asociarlo con una cuenta de servicio. Esta cuenta de servicio debe tener una función personalizada con permisos para gestionar recursos en Google Cloud.

[Configure una cuenta de servicio para el conector.](#)

- Si va a implementar Cloud Volumes ONTAP en varios proyectos, asegúrese de que el conector tiene acceso a dichos proyectos.

[Configure permisos en todos los proyectos.](#)

- Si utiliza un VPC compartido, configure los permisos en el proyecto de servicio y en el proyecto de host.

[Configure los permisos VPC compartidos.](#)

2

### Configure las redes

Se necesita un VPC y una subred con acceso de salida a Internet hacia extremos específicos. Si se requiere un servidor proxy para Internet de salida, necesitará la dirección IP, las credenciales y el certificado HTTPS.

[Ver los requisitos de red.](#)

3

### Habilite las API de Google Cloud

- 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)

4

### Cree el conector

Haga clic en el menú desplegable conector, seleccione **Agregar conector** y siga las indicaciones.

[Siga las instrucciones paso a paso.](#)

## Configure los permisos

Se requieren permisos para lo siguiente:

- El usuario que desplegará el conector VM
- Una cuenta de servicio que necesita conectar a la máquina virtual del conector durante la implementación

Según la configuración existente, es posible que deba realizar también los siguientes pasos:

- Configure permisos en todos los proyectos
- Configurar permisos para un VPC compartido

## Configure los permisos para desplegar el conector

Antes de implementar un conector, debe asegurarse de que su cuenta de Google Cloud tiene los permisos correctos.

### Pasos

1. "Crear una función personalizada" esto incluye los siguientes permisos:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
```



- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `resourcemanager.projects.get`
- `compute.instances.setServiceAccount`
- `iam.serviceAccounts.list`

2. Adjunte la función personalizada al usuario que implementará Connector desde BlueXP.

## Resultado

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

## Configure una cuenta de servicio para el conector

Se requiere una cuenta de servicio para proporcionar al conector el permiso que necesita para gestionar recursos en Google Cloud. Asociará esta cuenta de servicio con el conector VM al crearla.

Los permisos para la cuenta de servicio son diferentes a los permisos que configuró en la sección anterior.

## Pasos

1. "Crear una función personalizada" esto incluye los siguientes permisos:

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
```

- `compute.networks.updatePolicy`
- `compute.backendServices.create`
- `compute.addresses.list`
- `compute.disks.create`
- `compute.disks.createSnapshot`
- `compute.disks.delete`
- `compute.disks.get`
- `compute.disks.list`
- `compute.disks.setLabels`
- `compute.disks.use`
- `compute.firewalls.create`
- `compute.firewalls.delete`
- `compute.firewalls.get`
- `compute.firewalls.list`
- `compute.globalOperations.get`
- `compute.images.get`
- `compute.images.getFromFamily`
- `compute.images.list`
- `compute.images.useReadOnly`
- `compute.instances.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.instanceGroups.get`
- `compute.addresses.get`
- `compute.instances.updateNetworkInterface`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`

- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `compute.instances.setServiceAccount`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `logging.logEntries.list`
- `logging.privateLogEntries.list`
- `resourcemanager.projects.get`
- `storage.buckets.create`
- `storage.buckets.delete`
- `storage.buckets.get`
- `storage.buckets.list`
- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`
- `storage.buckets.update`
- `iam.serviceAccounts.getIamPolicy`
- `iam.serviceAccounts.list`
- `storage.objects.get`
- `storage.objects.list`
- `monitoring.timeSeries.list`
- `storage.buckets.getIamPolicy`
- `cloudkms.cryptoKeys.getIamPolicy`

- `cloudkms.cryptoKeys.setIamPolicy`
- `cloudkms.keyRings.get`
- `cloudkms.keyRings.getIamPolicy`
- `cloudkms.keyRings.setIamPolicy`

2. "Cree una cuenta de servicio de Google Cloud y aplique la función personalizada que acaba de crear".
3. Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, "Conceda acceso agregando la cuenta de servicio con la función BlueXP a ese proyecto". Deberá repetir este paso con cada proyecto.

## Resultado

Se ha configurado la cuenta de servicio del conector VM.

## Configure permisos en todos los proyectos

Si planea implementar sistemas Cloud Volumes ONTAP en proyectos diferentes a los del proyecto en el que reside el conector, tendrá que proporcionar a la cuenta de servicio del conector acceso a dichos proyectos.

Por ejemplo, supongamos que el conector está en el proyecto 1 y que desea crear sistemas Cloud Volumes ONTAP en el proyecto 2. Tendrá que otorgar acceso a la cuenta de servicio en el proyecto 2.

## Pasos

1. En la consola de Google Cloud, vaya al servicio IAM y seleccione el proyecto en el que desea crear sistemas Cloud Volumes ONTAP.
2. En la página **IAM**, seleccione **conceder acceso** y proporcione la información necesaria.
  - Introduzca el correo electrónico de la cuenta de servicio del conector.
  - Seleccione el rol personalizado del conector.
  - Haga clic en **Guardar**.

Para obtener información detallada, consulte "[Documentación de Google Cloud](#)"

## Configure los permisos VPC compartidos

Si se utiliza un VPC compartido para implementar recursos en un proyecto de servicio, se requieren los siguientes permisos. Esta tabla es de referencia y el entorno debe reflejar la tabla de permisos cuando se haya completado la configuración de IAM.

Identidad	Creador	Alojadas en	Permisos de proyecto de servicio	Permisos del proyecto host	Específico
Cuenta de Google utilizada para desplegar el conector	Personalizado	Proyecto de servicio	<ul style="list-style-type: none"> <li>• "<a href="#">Los permisos encontrados en esta sección anterior</a>"</li> </ul>	<ul style="list-style-type: none"> <li>• compute.networkUser</li> </ul>	Despliegue del conector en el proyecto de servicio

Identidad	Creador	Alojadas en	Permisos de proyecto de servicio	Permisos del proyecto host	Específico
Cuenta de servicio del conector	Personalizado	Proyecto de servicio	<ul style="list-style-type: none"> <li>"<a href="#">Los permisos encontrados en esta sección anterior</a>"</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> <li>deploymentmanager.editor</li> </ul>	Implementación y mantenimiento de Cloud Volumes ONTAP y servicios en el proyecto de servicio
Cuenta de servicio de Cloud Volumes ONTAP	Personalizado	Proyecto de servicio	<ul style="list-style-type: none"> <li>storage.admin</li> <li>miembro: Cuenta de servicio de BlueXP como serviceAccount.user</li> </ul>	N.A.	(Opcional) para la organización en niveles de datos y Cloud Backup
Agente de servicio de API de Google	Google Cloud	Proyecto de servicio	<ul style="list-style-type: none"> <li>(Predeterminado) Editor</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	Interactúa con las API de Google Cloud en nombre de la implementación. Permite a BlueXP utilizar la red compartida.
Cuenta de servicio predeterminada de Google Compute Engine	Google Cloud	Proyecto de servicio	<ul style="list-style-type: none"> <li>(Predeterminado) Editor</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	Pone en marcha instancias de Google Cloud e infraestructura de computación en nombre de la puesta en marcha. Permite a BlueXP utilizar la red compartida.

#### Notas:

1. deploymentmanager.editor sólo es necesario en el proyecto host si no pasa reglas de firewall a la implementación y decide dejar que BlueXP las cree por usted. BlueXP creará una implementación en el proyecto host que contiene la regla de firewall VPC0 si no se especifica ninguna regla.
2. Firewall.create y firewall.delete sólo son necesarios si no está pasando reglas de firewall a la implementación y está eligiendo permitir que BlueXP las cree para usted. Estos permisos residen en el archivo .yaml de cuenta de BlueXP. Si va a implementar un par de alta disponibilidad mediante un VPC compartido, estos permisos se utilizarán para crear las reglas de firewall para VPC1, 2 y 3. Para todas las demás implementaciones, estos permisos también se utilizarán para crear reglas para VPC0.
3. Para la organización en niveles de los datos, la cuenta del servicio de organización en niveles debe tener el rol serviceAccount.user en la cuenta de servicio, no solo en el nivel del proyecto. Actualmente, si asigna serviceAccount.user en el nivel de proyecto, los permisos no se muestran cuando consulta la cuenta de servicio con getIAMPolicy.

## Configure las redes

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.

### Conexión a redes de destino

Un conector requiere una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que tiene previsto habilitar.

Por ejemplo, si instala un conector en su red corporativa, debe configurar una conexión VPN a la red virtual en la que inicie Cloud Volumes ONTAP.

### Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública.

Puntos finales	Específico
<a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> <a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a> <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> <a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a>	Para gestionar recursos en Google Cloud.
<a href="https://support.netapp.com">https://support.netapp.com</a>	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
<a href="https://*.api.bluelxp.netapp.com">https://*.api.bluelxp.netapp.com</a> <a href="https://api.bluelxp.netapp.com">https://api.bluelxp.netapp.com</a> <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	<div><div>Proporcionar funciones y servicios SaaS dentro de BlueXP.</div><div><div>El conector se está comunicando actualmente con "cloudmanager.cloud.netapp.com" pero empezará a ponerse en contacto con "api.bluelxp.netapp.com" en una próxima versión.</div></div></div>
<a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	Para actualizar el conector y sus componentes de Docker.

### Servidor proxy

Si su organización requiere la implementación de un servidor proxy para todo el tráfico saliente de Internet, obtenga la siguiente información acerca del proxy HTTP o HTTPS:

- Dirección IP
- Credenciales

- Certificado HTTPS

## Grupo de seguridad

No hay tráfico entrante en el conector, a menos que lo inicie o si el conector se utiliza como proxy para los mensajes AutoSupport. HTTP y HTTPS proporcionan acceso al ["Interfaz de usuario local"](#), que utilizará en raras circunstancias. SSH solo es necesario si necesita conectarse al host para la solución de problemas.

## Limitación de dirección IP

Puede haber un conflicto con las direcciones IP en el rango 172. ["Obtenga más información sobre esta limitación"](#).

## Habilite las API de Google Cloud

Se necesitan varias API para implementar el conector y Cloud Volumes ONTAP.

### Paso

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

## Cree un conector

Cree un conector en Google Cloud directamente desde la interfaz de usuario de BlueXP o utilizando gcloud.

## BlueXP

1. Si está creando su primer entorno de trabajo, haga clic en **Agregar entorno de trabajo** y siga las indicaciones. De lo contrario, haga clic en el menú desplegable **conector** y seleccione **Agregar conector**.



2. Elija **Google Cloud Platform** como su proveedor de cloud.
3. En la página **despliegue de un conector**, revise los detalles sobre lo que necesitará. Dispone de dos opciones:
  - a. Haga clic en **continuar** para preparar la implementación utilizando la guía del producto. Cada paso de la guía del producto incluye la información que se incluye en esta página de la documentación.
  - b. Haga clic en **Ir a implementación** si ya ha preparado siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el conector:
  - Si se le solicita, inicie sesión en su cuenta de Google, que debería tener los permisos necesarios para crear la instancia de la máquina virtual.

El formulario es propiedad de Google y está alojado en él. Sus credenciales no se proporcionan a NetApp.

- **Detalles:** Introduzca un nombre para la instancia de la máquina virtual, especifique etiquetas, seleccione un proyecto y, a continuación, seleccione la cuenta de servicio que tenga los permisos necesarios (consulte la sección anterior para obtener más información).
  - **ubicación:** Especifique una región, zona, VPC y subred para la instancia.
  - **Red:** Elija si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
  - **Directiva de firewall:** Elija si desea crear una nueva directiva de firewall o si desea seleccionar una directiva de firewall existente que permita el acceso entrante HTTP, HTTPS y SSH.
  - **Revisión:** Revise sus selecciones para verificar que su configuración es correcta.
5. Haga clic en **Agregar**.

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

gcloud



1. Inicie sesión en el SDK de gcloud con su metodología preferida.

En nuestros ejemplos, utilizaremos un shell local con gcloud SDK instalado, pero puede utilizar Google Cloud Shell nativo en la consola de Google Cloud.

Para obtener más información acerca de Google Cloud SDK, visite la ["Página de documentación de Google Cloud SDK"](#).

2. Compruebe que ha iniciado sesión como usuario que tiene los permisos necesarios definidos en la sección anterior:

```
gcloud auth list
```

El resultado debe mostrar lo siguiente en el que la cuenta de usuario \* es la cuenta de usuario que desea iniciar sesión como:

```
Credentialed Accounts
ACTIVE  ACCOUNT
      some_user_account@domain.com
*      desired_user_account@domain.com
To set the active account, run:
$ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Ejecute el `gcloud compute instances create` comando:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

**nombre-instancia**

El nombre de la instancia de máquina virtual que desee para la instancia de.

**proyecto**

(Opcional) el proyecto en el que desea poner en marcha la máquina virtual.

**cuenta de servicio**

La cuenta de servicio especificada en la salida del paso 2.

**zona**

La zona en la que desea implementar la máquina virtual

**sin dirección**

(Opcional) no se utiliza ninguna dirección IP externa (se necesita un NAT o un proxy en la nube para enrutar el tráfico a Internet pública)

**etiqueta de red**

(Opcional) Agregar etiquetado de red para vincular una regla de firewall mediante etiquetas a la instancia de conector

**ruta de la red**

(Opcional) Añada el nombre de la red a la cual implementar el conector en (para un VPC compartido, se necesita la ruta completa)

**ruta de subred**

(Opcional) Añada el nombre de la subred en la que se va a implementar el conector (para un VPC compartido, se necesita la ruta completa)

**km-clave-ruta**

(Opcional) Agregar una clave KMS para cifrar los discos del conector (también es necesario aplicar permisos IAM)

Para obtener más información acerca de estas marcas, visite ["Documentación sobre Google Cloud Computing SDK"](#).

+

Al ejecutar el comando se pone en marcha el conector con la imagen maestra de NetApp. La instancia y el software del conector deben estar funcionando en aproximadamente cinco minutos.

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

`https://ipaddress[]`

2. Después de iniciar sesión, configure el conector:
  - a. Especifique la cuenta de NetApp que desea asociar al conector.  
  
["Obtenga más información acerca de las cuentas de NetApp"](#).
  - b. Escriba un nombre para el sistema.

## Resultado

El conector ahora está instalado y configurado con su cuenta de NetApp. BlueXP utilizará este conector automáticamente cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará ["alterne entre ellos"](#).

Si tiene cubos de Google Cloud Storage en la misma cuenta de Google Cloud en la que creó el conector, verá que aparece un entorno de trabajo de Google Cloud Storage en el lienzo automáticamente. ["Obtenga más información sobre lo que puede hacer con este entorno de trabajo"](#).

## Abra el puerto 3128 para los mensajes de AutoSupport

Si tiene previsto implementar sistemas Cloud Volumes ONTAP en una subred en la que no esté disponible una conexión a Internet saliente, BlueXP configura automáticamente Cloud Volumes ONTAP para que utilice el conector como servidor proxy.

El único requisito es asegurarse de que el grupo de seguridad del conector permita conexiones *entrante* a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Si utiliza el grupo de seguridad predeterminado para Cloud Volumes ONTAP, no es necesario realizar cambios en su grupo de seguridad. Pero si tiene pensado definir reglas de salida estrictas para Cloud Volumes ONTAP, también tendrá que asegurarse de que el grupo de seguridad Cloud Volumes ONTAP permita conexiones *saliente* a través del puerto 3128.

## Cree un conector en una región gubernamental

Si trabaja en una región gubernamental, necesita implementar un conector desde el mercado de su proveedor de cloud o instalar manualmente el software del conector en un host Linux existente. No puede desplegar el conector en una región gubernamental desde el sitio web de BlueXP SaaS.

Utilice uno de los siguientes vínculos para ver las instrucciones para crear un conector:

- ["Cree un conector desde AWS Marketplace"](#)
- ["Cree un conector y un Cloud Volumes ONTAP en el entorno AWS C2S"](#)
- ["Cree un conector desde Azure Marketplace"](#)
- ["Instale un conector en su propio host Linux"](#)

Para las instalaciones manuales en su propio host Linux, debe utilizar el instalador "online" para instalar el conector en un host que tenga acceso a Internet. Hay disponible un instalador independiente "offline" para el conector, pero sólo es compatible con sitios locales que no tienen acceso a Internet. No cuenta con soporte para regiones gubernamentales.

Después de desplegar el conector, puede acceder a BlueXP abriendo el explorador Web y conectándose a la dirección IP de la instancia de conector: `https://ipaddress[]`

Dado que el conector se desplegó en una región gubernamental, no se puede acceder a él desde <https://console.bluexp.netapp.com>.

## Información de copyright

Copyright © 2023 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 INTERRUPCIÓN 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.