Cree un conector

BlueXP setup and administration

NetApp
May 20, 2025

Tabla de contenidos

Cree un conector

AWS

Opciones de instalación de conectores en AWS

Hay varias formas diferentes de crear un conector en AWS. Directamente desde BlueXP es la forma más común.

Están disponibles las siguientes opciones de instalación:

- "Crea el conector directamente desde BlueXP" (esta es la opción estándar)

  Esta acción inicia una instancia de EC2 con Linux y el software Connector en un VPC de su elección.

- "Cree un conector desde AWS Marketplace"

  Esta acción también inicia una instancia de EC2 que ejecuta Linux y el software Connector, pero la puesta en marcha se inicia directamente desde AWS Marketplace en lugar de desde BlueXP.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará a la forma en que se prepara para la instalación. Esto incluye cómo proporciona BlueXP los permisos necesarios para autenticar y gestionar recursos en AWS.

Cree un conector en AWS desde BlueXP

Puede crear un conector en AWS directamente desde BlueXP . Para crear un conector en AWS desde BlueXP, debe configurar la red, preparar los permisos de AWS y, a continuación, crear el conector.

Antes de empezar

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

Paso 1: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

VPC y subred

Al crear el conector, es necesario especificar el VPC y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

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

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

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

Extremos en los que se han contactado desde la consola de BlueXP

A medida que utiliza la consola basada en Web BlueXP que se proporciona a través de la capa SaaS, se pone en contacto con varios extremos para completar las tareas de gestión de datos. Esto incluye los extremos que se ponen en contacto para poner en marcha el conector desde la consola de BlueXP.

"Consulte la lista de extremos con los que se ha contactado desde la consola de BlueXP".

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras circunstancias.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Configure los permisos de AWS

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

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

Con cualquiera de las dos opciones, el primer paso es crear una política de IAM. Esta directiva sólo contiene los permisos necesarios para iniciar la instancia de Connector en AWS desde BlueXP.

Si es necesario, puede restringir la política de IAM mediante el IAM `Condition` elemento. "Documentación de AWS: Elemento de condición"

Pasos

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

   Esta directiva sólo contiene los permisos necesarios para iniciar la instancia de Connector en AWS desde BlueXP. Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos a la instancia de Connector que permite al conector gestionar recursos de AWS. "Permite ver los permisos necesarios para la propia instancia del conector".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
```

```
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/OCCMInstance": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
```

```
        ]
      }
    ]
}
```

5. Seleccione **Siguiente** y agregue etiquetas, si es necesario.
6. Selecciona **Siguiente** e introduce un nombre y una descripción.
7. Seleccione **Crear política**.
8. Adjunte la política a una función de IAM que BlueXP puede asumir o a un usuario de IAM para que pueda proporcionar claves de acceso a BlueXP:
   - (Opción 1) Configurar una función de IAM que BlueXP puede asumir:
     i. Vaya a la consola AWS IAM de la cuenta de destino.
     ii. En Access Management, seleccione **roles > Crear función** y siga los pasos para crear la función.
     iii. En **Tipo de entidad de confianza**, seleccione **cuenta de AWS**.
     iv. Seleccione **otra cuenta de AWS** e introduzca el ID de la cuenta de BlueXP SaaS: 952013314444
     v. Seleccione la directiva que ha creado en la sección anterior.
     vi. Después de crear la función, copie la función ARN para que pueda pegarla en BlueXP al crear el conector.
   - (Opción 2) Configurar permisos para un usuario de IAM para que pueda proporcionar claves de acceso a BlueXP:
     i. Desde la consola de AWS IAM, seleccione **Usuarios** y, a continuación, seleccione el nombre de usuario.
     ii. Selecciona **Añadir permisos > Adjuntar políticas existentes directamente**.
     iii. Seleccione la política que ha creado.
     iv. Seleccione **Siguiente** y luego seleccione **Agregar permisos**.
     v. Asegúrese de disponer de la clave de acceso y la clave secreta para el usuario del IAM.

Resultado

Ahora debe tener un rol de IAM que tenga los permisos necesarios o un usuario de IAM que tenga los permisos necesarios. Al crear el conector desde BlueXP, puede proporcionar información sobre la función o las claves de acceso.

Paso 3: Crear el conector

Crea el Connector directamente desde la consola basada en web de BlueXP.

Acerca de esta tarea

- Al crear el conector desde BlueXP se implementa una instancia de EC2 en AWS con una configuración predeterminada. Después de crear el conector, no debe cambiar a un tipo de instancia EC2 más pequeño que tenga menos CPU o RAM. "Obtenga información sobre la configuración predeterminada para el conector".
- Cuando BlueXP crea el conector, crea un rol de IAM y un perfil de instancia para la instancia. Este rol incluye permisos que permiten al conector administrar recursos de AWS. Debe asegurarse de que el rol se mantiene actualizado a medida que se agregan nuevos permisos en versiones posteriores. "Obtenga más información sobre la política de IAM para el conector".

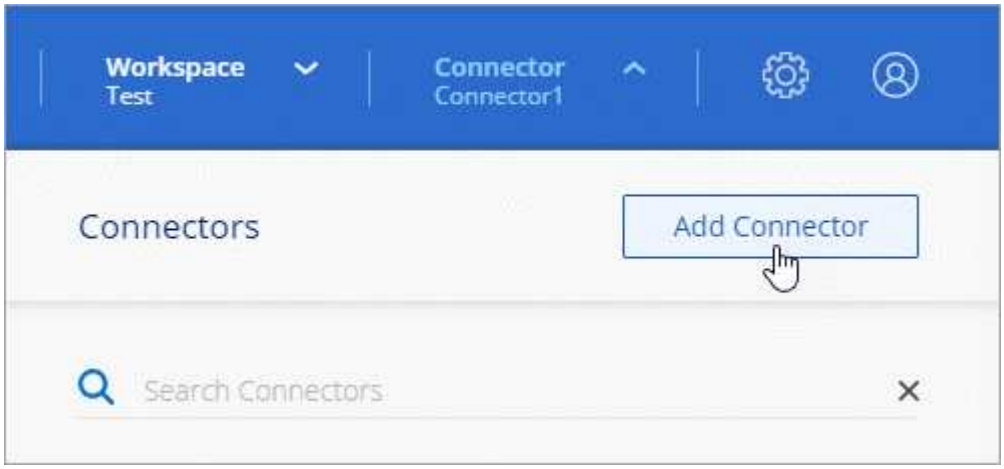
Antes de empezar

Debe tener lo siguiente:

- Un método de autenticación de AWS: Un rol de IAM o claves de acceso para un usuario IAM con los permisos necesarios.
- Un VPC y una subred que cumplan los requisitos de red.
- Una pareja de claves para la instancia de EC2.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector.

Pasos

1. Seleccione la lista desplegable **Connector** y seleccione **Add Connector**.



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

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

   - **Detalles**: Proporcione detalles sobre el conector.
     - Escriba un nombre para la instancia.
     - Añada etiquetas personalizadas (metadatos) a la instancia.

- Elija si desea que BlueXP cree una nueva función que tenga los permisos necesarios o si desea seleccionar una función existente con la que haya configurado "los permisos necesarios".
- Elija si desea cifrar los discos EBS del conector. Tiene la opción de utilizar la clave de cifrado predeterminada o utilizar una clave personalizada.

◦ **Red**: Especifique un VPC, una subred y un par de claves para la instancia, elija si desea habilitar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.

Asegúrese de que tiene el par de llaves correcto para usar con el conector. Sin un par de teclas, no podrá acceder a la máquina virtual conector.

◦ **Grupo de seguridad**: Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita las reglas entrantes y salientes requeridas.

"Ver reglas de grupos de seguridad para AWS".

◦ **Revisión**: Revise sus selecciones para verificar que su configuración es correcta.

5. Seleccione **Agregar**.

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

Resultado

Una vez completado el proceso, el conector está disponible para su uso en BlueXP.

Si tienes buckets de Amazon S3 en la misma cuenta de AWS en la que creaste el conector, verás que aparece automáticamente un entorno de trabajo de Amazon S3 en el lienzo de BlueXP. "Descubre cómo gestionar buckets S3 de BlueXP"

Cree un conector desde AWS Marketplace

Puede crear un conector en AWS directamente desde AWS Marketplace. Para crear un conector desde AWS Marketplace, debe configurar la red, preparar los permisos de AWS, revisar los requisitos de la instancia y, a continuación, crear el conector.

Antes de empezar

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

Paso 1: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

VPC y subred

Al crear el conector, es necesario especificar el VPC y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

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

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

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

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras circunstancias.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Configure los permisos de AWS

Para preparar una implementación de Marketplace, cree políticas de IAM en AWS y adjuntarlas a una función de IAM. Al crear el conector desde AWS Marketplace, se le pedirá que seleccione ese rol de IAM.

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:

a. Selecciona **Políticas > Crear política**.

b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".

c. Finalice los pasos restantes para crear la directiva.

Dependiendo de los servicios de BlueXP que tenga previsto utilizar, puede que necesite crear una segunda política. Para las regiones estándar, los permisos se distribuyen en dos directivas. Son necesarias dos políticas debido a un límite máximo de tamaño de carácter para las políticas gestionadas en AWS. "Obtenga más información sobre las políticas de IAM para el conector".

3. Cree un rol IAM:

a. Selecciona **Roles > Crear rol**.

b. Seleccione **Servicio AWS > EC2**.

c. Agregue permisos asociando la directiva que acaba de crear.

d. Finalice los pasos restantes para crear la función.

Resultado

Ahora tiene el rol de IAM que se puede asociar a la instancia de EC2 durante la implementación desde AWS Marketplace.

Paso 3: Revise los requisitos de la instancia

Al crear el conector, debe elegir un tipo de instancia EC2 que cumpla los siguientes requisitos.

CPU

8 núcleos o 8 vCPU

RAM

32GB

Tipo de instancia de AWS EC2

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

Paso 4: Crear el conector

Cree el conector directamente desde AWS Marketplace.

Acerca de esta tarea

Al crear el conector desde AWS Marketplace se implementa una instancia EC2 en AWS con una configuración predeterminada. "Obtenga información sobre la configuración predeterminada para el conector".

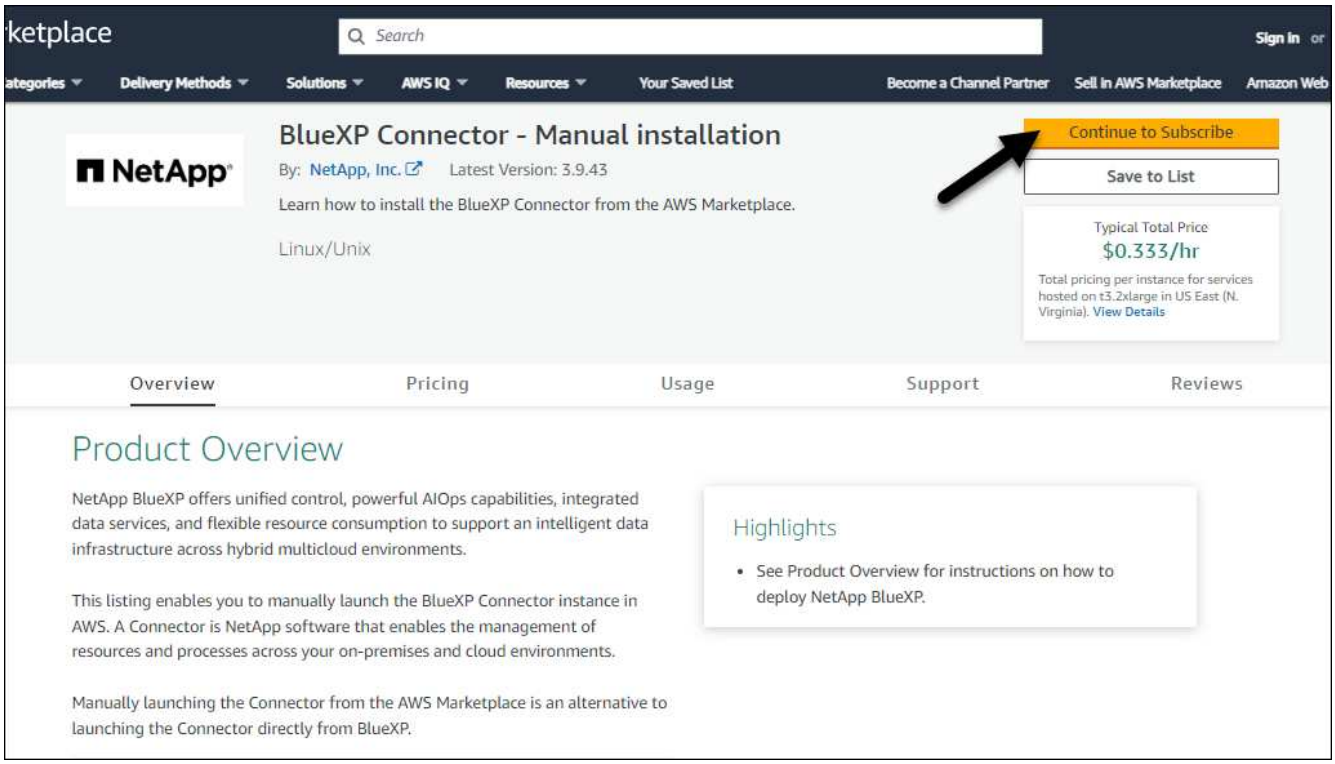
Antes de empezar

Debe tener lo siguiente:

- Un VPC y una subred que cumplan los requisitos de red.
- Función IAM con una directiva adjunta que incluye los permisos necesarios para el conector.
- Permisos para suscribirse y cancelar la suscripción a AWS Marketplace para su usuario de IAM.
- Comprensión de los requisitos de CPU y RAM para la instancia.
- Una pareja de claves para la instancia de EC2.

Pasos

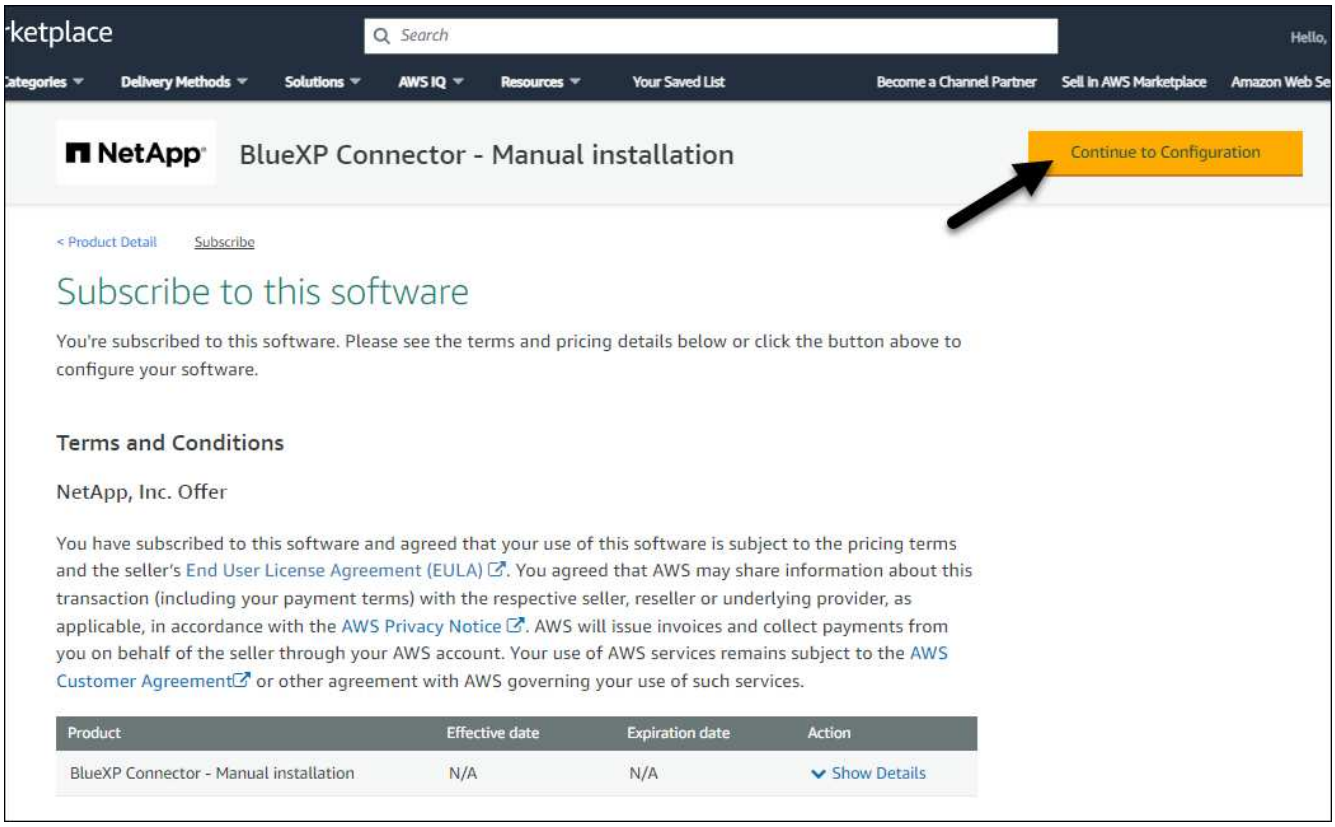
1. Vaya a la "Lista del conector BlueXP en el AWS Marketplace"
2. En la página de Marketplace, selecciona **Continuar para suscribirte**.



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

   El proceso de suscripción puede tardar unos minutos.

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



5. En la página **Configurar este software**, asegúrate de haber seleccionado la región correcta y luego selecciona **Continuar para iniciar**.
6. En la página **Iniciar este software**, en **Elegir acción**, selecciona **Iniciar a través de EC2** y luego selecciona **Iniciar**.

   Estos pasos describen cómo iniciar la instancia desde la consola EC2 porque la consola permite asociar una función IAM a la instancia del conector. Esto no es posible usando la acción **Iniciar desde el sitio web**.

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

   - **Nombre y etiquetas**: Introduzca un nombre y etiquetas para la instancia.
   - **Aplicaciones e imágenes del sistema operativo**: Omita esta sección. El conector AMI ya está seleccionado.
   - **Tipo de instancia**: Dependiendo de la disponibilidad de la región, elija un tipo de instancia que cumpla con los requisitos de RAM y CPU (t3,2xlarge está preseleccionado y recomendado).
   - **Par de claves (login)**: Seleccione el par de claves que desea utilizar para conectarse de forma segura a la instancia.
   - **Ajustes de red**: Edite los ajustes de red según sea necesario:
     - Elija el VPC y la subred que desee.
     - Especifique si la instancia debe tener una dirección IP pública.
     - Especifique la configuración del grupo de seguridad que habilite los métodos de conexión necesarios para la instancia de conector: SSH, HTTP y HTTPS.

       "Ver reglas de grupos de seguridad para AWS".

- **Configurar almacenamiento**: Mantenga el tamaño predeterminado y el tipo de disco para el volumen raíz.

  Si desea habilitar el cifrado de Amazon EBS en el volumen raíz, seleccione **Avanzado**, expanda **Volumen 1**, seleccione **Cifrado** y, a continuación, elija una clave KMS.

- **Detalles avanzados**: En **perfil de instancia de IAM**, elija la función de IAM que incluye los permisos necesarios para el conector.
- **Resumen**: Revisa el resumen y selecciona **Iniciar Instancia**.

AWS inicia el software con la configuración especificada. La instancia y el software del conector deben estar funcionando en aproximadamente cinco minutos.

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

   https://ipaddress

9. Después de iniciar sesión, configure el conector:
   a. Especifique la organización BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y configurado con su organización BlueXP .

Abra un explorador web y vaya al "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Si tienes buckets de Amazon S3 en la misma cuenta de AWS en la que creaste el conector, verás que aparece automáticamente un entorno de trabajo de Amazon S3 en el lienzo de BlueXP. "Descubre cómo gestionar buckets S3 de BlueXP"

Instale manualmente el conector en AWS

Puede instalar manualmente un conector en un host Linux ejecutándose en AWS. Para instalar manualmente Connector en su propio host Linux, debe revisar los requisitos del host, configurar la red, preparar los permisos de AWS, instalar Connector y, a continuación, proporcionar los permisos que preparó.

Antes de empezar

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

Paso 1: Revise los requisitos del host

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

Host dedicado

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

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

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

Hipervisor

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

Requisitos del sistema operativo y del contenedor

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

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Docker Engine 26.0.0	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros necesario durante la instalación del conector.

Tipo de instancia de AWS EC2

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

Par de claves

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

Límite de salto de respuesta PUT al usar IMDSv2

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

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

Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

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

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

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

Paso 2: Instale Podman o Docker Engine

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

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

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 1. Pasos

Podman

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

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

Pasos

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

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

2. Instale Podman.

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

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

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

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

3. Active e inicie el servicio podman.socket.

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

4. Instale python3.

```
sudo dnf install python3
```

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

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

Para Red Hat Enterprise Linux 9:

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

Para Red Hat Enterprise Linux 8:

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

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

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

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

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

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

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 3: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde los equipos cuando se utiliza la consola basada en web de BlueXP

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

"Prepare las redes para la consola de BlueXP ".

Puntos finales contactados durante la instalación manual

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

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

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

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

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

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

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

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.

- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras circunstancias.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Paso 4: Configurar permisos

Necesitas proporcionar permisos de AWS a BlueXP mediante una de las siguientes opciones:

- Opción 1: Crear políticas IAM y asociar las políticas a una función IAM que se puede asociar a la instancia de EC2.
- Opción 2: Proporcione a BlueXP la clave de acceso de AWS para un usuario de IAM que tenga los permisos requeridos.

Sigue los pasos para preparar permisos para BlueXP.

Rol IAM

Pasos

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

      Dependiendo de los servicios de BlueXP que tenga previsto utilizar, puede que necesite crear una segunda política. Para las regiones estándar, los permisos se distribuyen en dos directivas. Son necesarias dos políticas debido a un límite máximo de tamaño de carácter para las políticas gestionadas en AWS. "Obtenga más información sobre las políticas de IAM para el conector".
3. Cree un rol IAM:
   a. Selecciona **Roles > Crear rol**.
   b. Seleccione **Servicio AWS > EC2**.
   c. Agregue permisos asociando la directiva que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

Resultado

Ahora tiene la función IAM que puede asociar con la instancia de EC2 después de instalar el conector.

Clave de acceso de AWS

Pasos

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

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

   Para las regiones estándar, los permisos se distribuyen en dos directivas. Son necesarias dos políticas debido a un límite máximo de tamaño de carácter para las políticas gestionadas en AWS. "Obtenga más información sobre las políticas de IAM para el conector".
3. Adjunte las políticas a un usuario de IAM.
   - "Documentación de AWS: Crear roles de IAM"
   - "Documentación de AWS: Adición y eliminación de políticas de IAM"
4. Asegúrese de que el usuario tiene una clave de acceso que puede agregar a BlueXP después de instalar el conector.

Resultado

Ahora dispone de un usuario de IAM que tiene los permisos necesarios y una clave de acceso que puede

proporcionar a BlueXP.

Paso 5: Instale el conector

Una vez completados los requisitos previos, puede instalar manualmente el software en su propio host Linux.

Antes de empezar

Debe tener lo siguiente:

- Privilegios de root para instalar el conector.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector.

  Tiene la opción de configurar un servidor proxy después de la instalación, pero para hacerlo es necesario reiniciar el conector.

  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.

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.

5. Espere a que finalice la instalación.

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

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

https://ipaddress

7. Después de iniciar sesión, configure el conector:
   a. Especifique la organización BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y se configura con su organización BlueXP .

Si tienes buckets de Amazon S3 en la misma cuenta de AWS en la que creaste el conector, verás que aparece automáticamente un entorno de trabajo de Amazon S3 en el lienzo de BlueXP. "Descubre cómo gestionar buckets S3 de BlueXP"

Paso 6: Proporcionar permisos a BlueXP

Ahora que ha instalado Connector, debe proporcionar a BlueXP los permisos de AWS que configuró anteriormente. Al proporcionar los permisos, BlueXP podrá gestionar tus datos y la infraestructura de almacenamiento en AWS.

Rol IAM

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

Pasos

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

Resultado

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

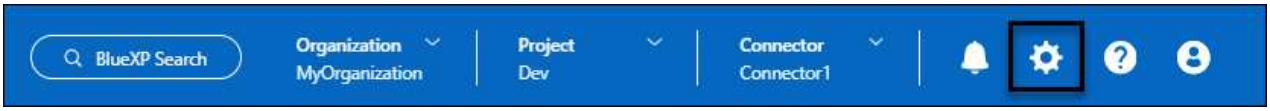
Vaya a la "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Clave de acceso de AWS

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

Pasos

1. Asegúrese de que el conector correcto está seleccionado actualmente en BlueXP.
2. En la parte superior derecha de la consola de BlueXP, seleccione el icono Configuración y seleccione **credenciales**.



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

Resultado

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

Vaya a la "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Azure

Opciones de instalación del conector en Azure

Hay varias formas diferentes de crear un conector en Azure. Directamente desde BlueXP es la forma más común.

Están disponibles las siguientes opciones de instalación:

- "Crea un conector directamente desde BlueXP" (esta es la opción estándar)

  Esta acción lanza una VM que ejecuta Linux y el software Connector en una vnet de su elección.

- "Cree un conector desde Azure Marketplace"

  Esta acción también inicia una máquina virtual que ejecuta Linux y el software Connector, pero la puesta en marcha se inicia directamente desde Azure Marketplace en lugar de desde BlueXP.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará a la forma en que se prepara para la instalación. Esto incluye cómo proporciona BlueXP los permisos necesarios para autenticar y gestionar recursos en Azure.

Cree un conector en Azure desde BlueXP

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

Antes de empezar

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

Paso 1: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

Región de Azure

Si utiliza Cloud Volumes ONTAP, el conector debe desplegarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que gestiona, o en el "Par de regiones de Azure" Para los sistemas Cloud Volumes ONTAP. Este requisito garantiza que se utilice una conexión de enlace privado de Azure entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas.

"Conozca cómo Cloud Volumes ONTAP utiliza un enlace privado de Azure"

Vnet y subred

Al crear el conector, debe especificar el vnet y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

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

- Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
- El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.

- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Extremos en los que se han contactado desde la consola de BlueXP

A medida que utiliza la consola basada en Web BlueXP que se proporciona a través de la capa SaaS, se pone en contacto con varios extremos para completar las tareas de gestión de datos. Esto incluye los extremos que se ponen en contacto para poner en marcha el conector desde la consola de BlueXP.

"Consulte la lista de extremos con los que se ha contactado desde la consola de BlueXP".

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras circunstancias.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Crear una política de implementación de Connector (rol personalizado)

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

Cree una función personalizada de Azure que pueda asignar a su cuenta de Azure o a un director de servicio de Microsoft Entra. BlueXP autentica con Azure y utiliza estos permisos para crear la instancia de Connector

en su nombre.

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

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

Pasos

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

> Este rol personalizado solo contiene los permisos necesarios para iniciar Connector VM en Azure desde BlueXP. No utilice esta política para otras situaciones. Cuando BlueXP crea el conector, aplica un nuevo conjunto de permisos a la máquina virtual de Connector que permite al conector gestionar los recursos de Azure.

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

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

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

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

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

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/read",

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

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

   ejemplo

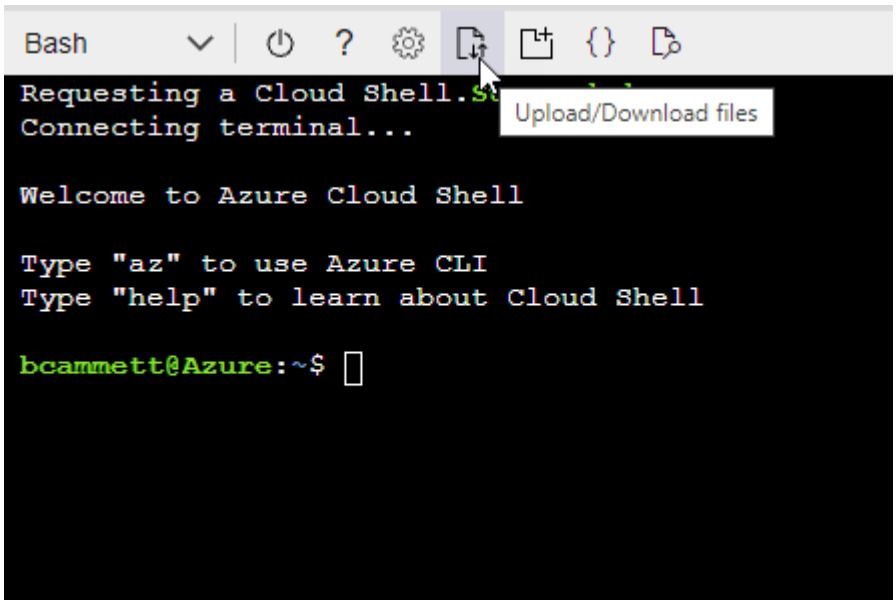
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
   ],
   ```

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

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

   a. Comenzar "Shell de cloud de Azure" Y seleccione el entorno Bash.

   b. Cargue el archivo JSON.

   c. Introduzca el siguiente comando CLI de Azure:

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

   Ahora debería tener una función personalizada denominada *Azure SetupAsService*. Ahora puede aplicar esta función personalizada a su cuenta de usuario o a un director de servicio.

Paso 3: Configurar la autenticación

Al crear el conector desde BlueXP, debes proporcionar un inicio de sesión que permita a BlueXP autenticarse con Azure y poner en marcha la máquina virtual. Dispone de dos opciones:

1. Inicie sesión con su cuenta de Azure cuando se le solicite. Esta cuenta debe tener permisos de Azure específicos. Esta es la opción predeterminada.
2. Proporcionar detalles acerca de un director de servicio de Microsoft Entra. Este principal de servicio

también requiere permisos específicos.

Sigue los pasos para preparar uno de estos métodos de autenticación para usarlos con BlueXP.

Cuenta de Azure

Asigne la función personalizada al usuario que implementará Connector desde BlueXP.

Pasos

1. En el portal de Azure, abra el servicio **Suscripciones** y seleccione la suscripción del usuario.
2. Haga clic en **Control de acceso (IAM)**.
3. Haga clic en **Agregar** > **Agregar asignación de rol** y, a continuación, agregue los permisos:
   a. Seleccione el rol **Azure SetupAsService** y haga clic en **Siguiente**.

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

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

Resultado

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

Director de servicios

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

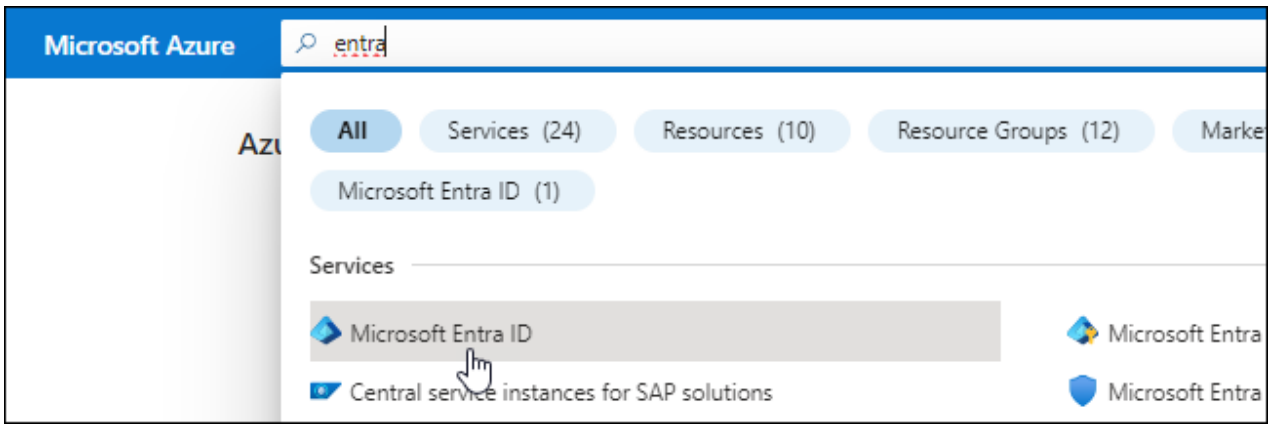
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

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

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

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

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



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

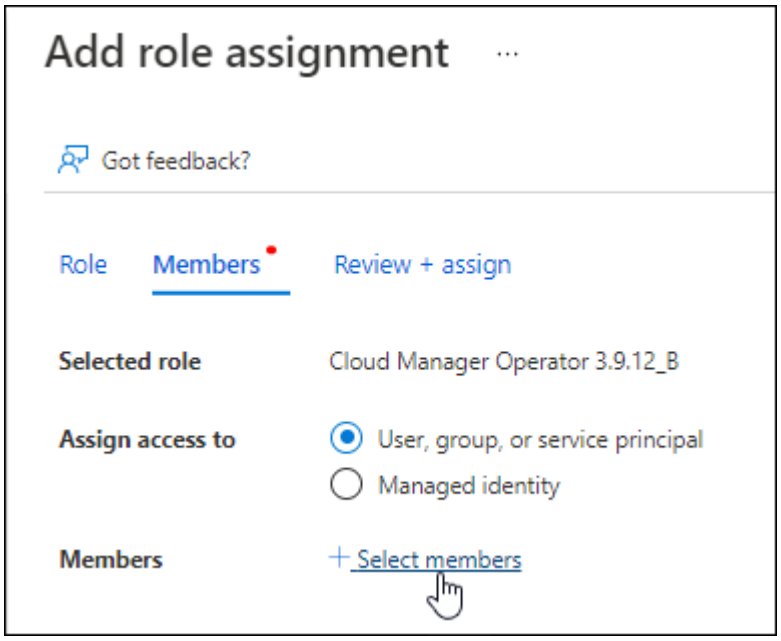
   Ha creado la aplicación AD y el director de servicio.

Asigne la función personalizada a la aplicación

1. En el portal de Azure, abra el servicio **Suscripciones**.
2. Seleccione la suscripción.
3. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
4. En la ficha **rol**, seleccione el rol **operador BlueXP** y haga clic en **Siguiente**.
5. En la ficha **Miembros**, realice los siguientes pasos:

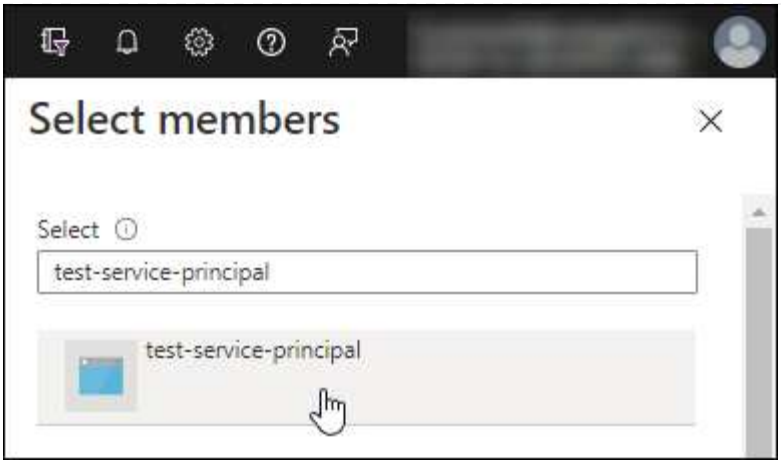
   a. Mantener seleccionado **Usuario, grupo o principal de servicio**.

   b. Haga clic en **Seleccionar miembros**.



   c. Busque el nombre de la aplicación.

   Veamos un ejemplo:



a. Seleccione la aplicación y haga clic en **Seleccionar**.

b. Haga clic en **Siguiente**.

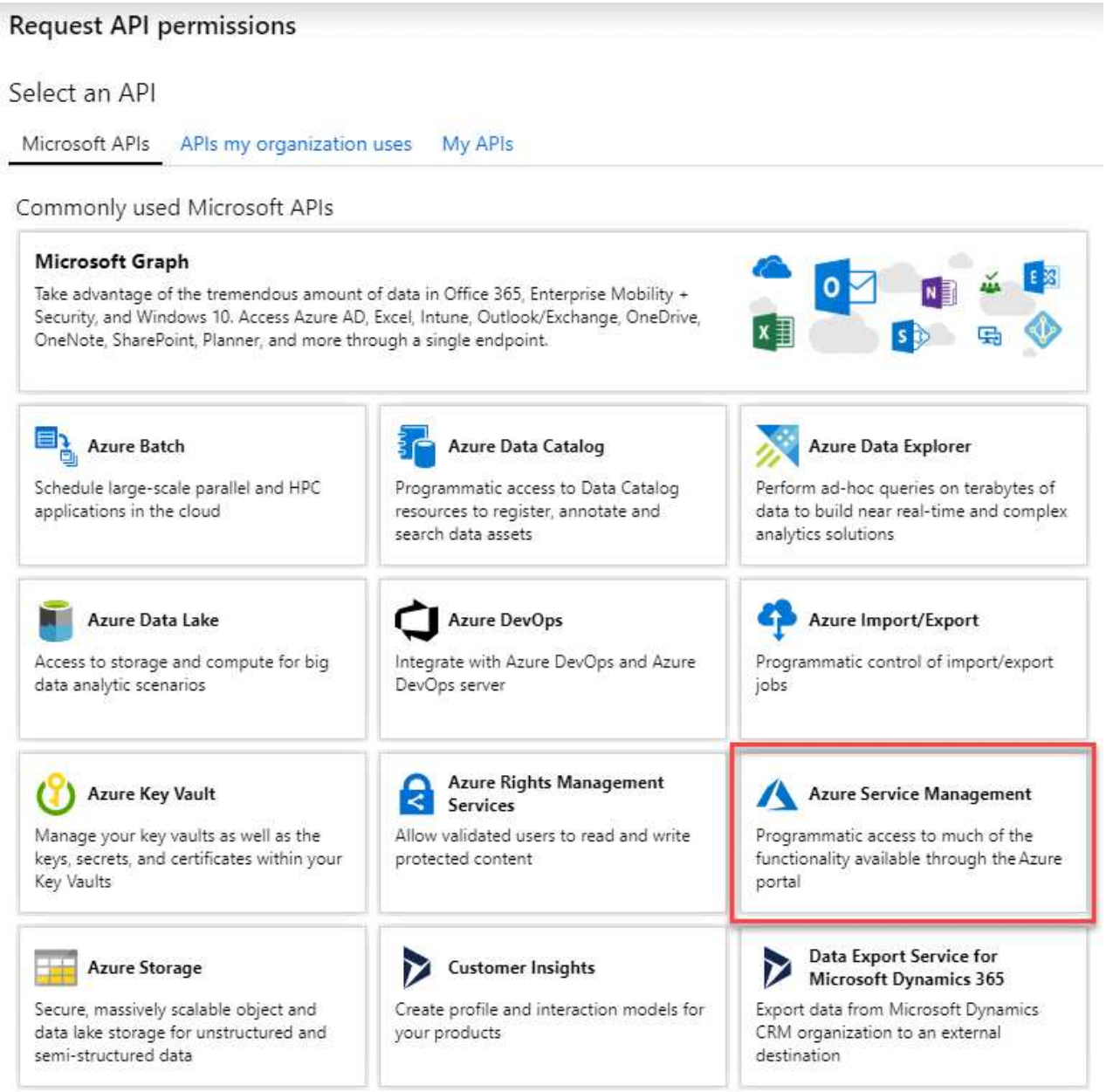
6. Haga clic en **revisar + asignar**.

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

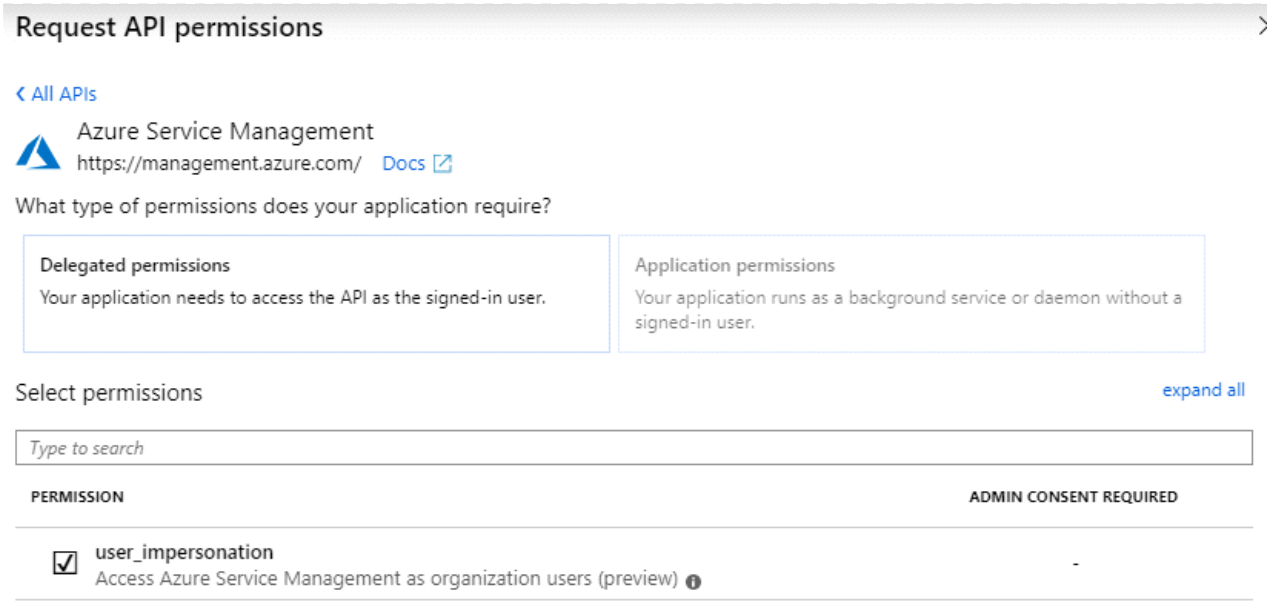
   Si desea administrar recursos en varias suscripciones de Azure, debe vincular el principal de servicio a cada una de esas suscripciones. Por ejemplo, BlueXP te permite seleccionar la suscripción que desees utilizar al implementar Cloud Volumes ONTAP.

Añada permisos de API de administración de servicios de Windows Azure

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

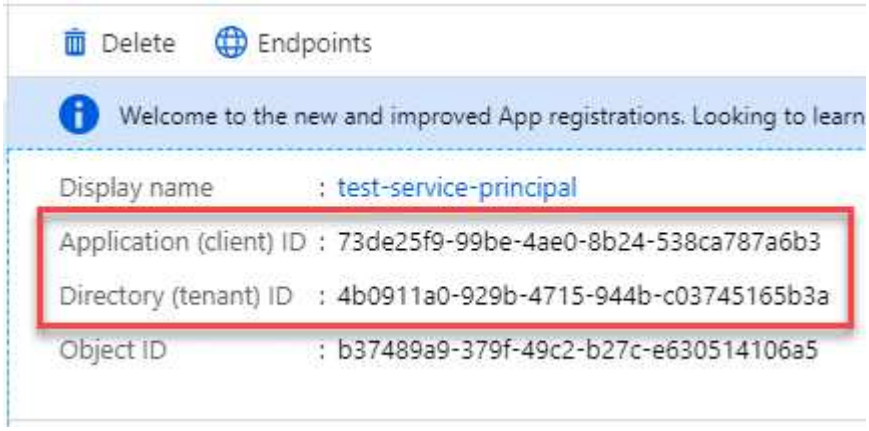


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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

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



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

Cree un secreto de cliente

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

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

Resultado

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

Paso 4: Crear el conector

Crea el Connector directamente desde la consola basada en web de BlueXP.

Acerca de esta tarea

- Al crear el conector desde BlueXP se implementa una máquina virtual en Azure con una configuración predeterminada. Después de crear el conector, no debe cambiar a un tipo de máquina virtual más pequeño que tenga menos CPU o RAM. "Obtenga información sobre la configuración predeterminada para el conector".
- Cuando BlueXP pone en marcha Connector, crea un rol personalizado y lo asigna a la máquina virtual Connector. Este rol incluye permisos que permiten al conector administrar recursos de Azure. Debe asegurarse de que el rol se mantiene actualizado a medida que se agregan nuevos permisos en versiones posteriores. "Obtenga más información sobre el rol personalizado del conector".

Antes de empezar

Debe tener lo siguiente:

- Una suscripción a Azure.
- Una red virtual y una subred en su región de Azure preferida.
- Detalles sobre un servidor proxy, si su empresa requiere un proxy para todo el tráfico saliente de Internet:
  - Dirección IP
  - Credenciales
  - Certificado HTTPS
- Una clave pública SSH, si desea utilizar ese método de autenticación para la máquina virtual Connector. La otra opción para el método de autenticación es usar una contraseña.

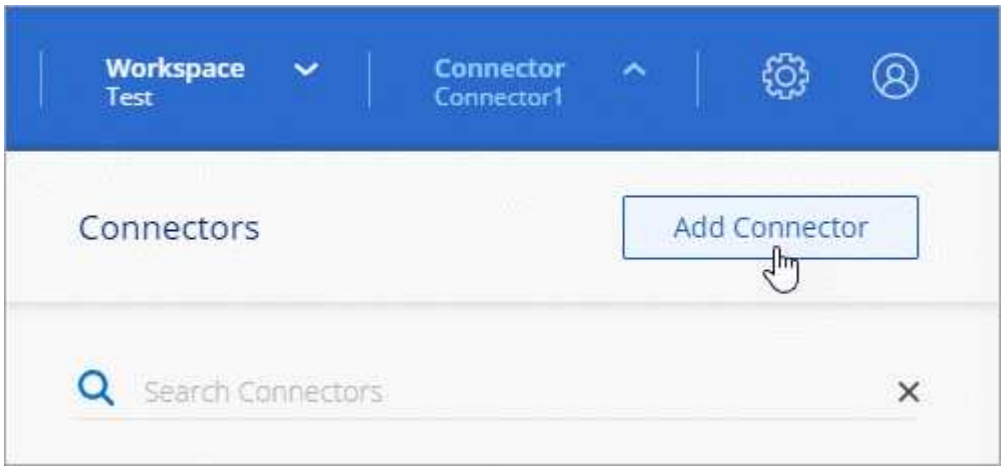
  "Obtenga más información sobre cómo conectarse a una máquina virtual de Linux en Azure"

- Si no quiere que BlueXP cree automáticamente una función de Azure para Connector, tendrá que crear la suya propia "uso de la política en esta página".

  Estos permisos son para la propia instancia de Connector. Se trata de un conjunto de permisos diferente al configurado anteriormente para implementar la VM de Connector.

Pasos

1. Seleccione la lista desplegable **Connector** y seleccione **Add Connector**.



2. Elija **Microsoft Azure** como proveedor de cloud.
3. En la página **despliegue de un conector**:

   a. En **autenticación**, seleccione la opción de autenticación que coincida con la forma en que configuró los permisos de Azure:

   - Seleccione **cuenta de usuario de Azure** para iniciar sesión en su cuenta de Microsoft, que debería tener los permisos necesarios.

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

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

   - Seleccione **Active Directory Service principal** para introducir información sobre el principal de servicio de Microsoft Entra que otorga los permisos necesarios:
     - ID de aplicación (cliente)
     - ID de directorio (inquilino)
     - Secreto de cliente

   Aprenda cómo obtener estos valores para un director de servicio.

4. Siga los pasos del asistente para crear el conector:

   ◦ **Autenticación de VM**: Elija una suscripción de Azure, una ubicación, un nuevo grupo de recursos o un grupo de recursos existente y, a continuación, elija un método de autenticación para la máquina virtual Connector que está creando.

   El método de autenticación para la máquina virtual puede ser una contraseña o una clave pública SSH.

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

- **Detalles**: Escriba un nombre para la instancia, especifique etiquetas y elija si desea que BlueXP cree una nueva función que tenga los permisos necesarios o si desea seleccionar una función existente con la que se haya configurado "los permisos necesarios".

  Tenga en cuenta que puede elegir las suscripciones de Azure asociadas a este rol. Cada suscripción que elija proporciona los permisos de Connector para administrar los recursos de esa suscripción (por ejemplo, Cloud Volumes ONTAP).

- **Red**: Elija un vnet y una subred, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
- **Grupo de seguridad**: Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita las reglas entrantes y salientes requeridas.

  "Ver reglas de grupo de seguridad para Azure".

- **Revisión**: Revise sus selecciones para verificar que su configuración es correcta.

5. Haga clic en **Agregar**.

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

Resultado

Una vez completado el proceso, el conector está disponible para su uso en BlueXP.

Si tienes almacenamiento de Azure Blob en la misma suscripción de Azure donde creaste el conector, verás que aparece automáticamente un entorno de trabajo de almacenamiento de Azure Blob en el lienzo de BlueXP. "Descubre cómo gestionar el almacenamiento de Azure Blob desde BlueXP"

Cree un conector desde Azure Marketplace

Puede crear un conector en Azure directamente desde Azure Marketplace. Para crear un conector desde Azure Marketplace, debe configurar su red, preparar los permisos de Azure, revisar los requisitos de la instancia y, a continuación, crear el conector.

Antes de empezar

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

Paso 1: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

Región de Azure

Si utiliza Cloud Volumes ONTAP, el conector debe desplegarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que gestiona, o en el "Par de regiones de Azure" Para los sistemas Cloud Volumes ONTAP. Este requisito garantiza que se utilice una conexión de enlace privado de Azure entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas.

"Conozca cómo Cloud Volumes ONTAP utiliza un enlace privado de Azure"

Vnet y subred

Al crear el conector, debe especificar el vnet y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

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

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

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras circunstancias.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Revise los requisitos de VM

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

CPU

8 núcleos o 8 vCPU

RAM

32GB

Tamaño de la máquina virtual de Azure

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

Paso 3: Configurar permisos

Puede proporcionar permisos de las siguientes maneras:

- Opción 1: Asigne un rol personalizado a la máquina virtual de Azure mediante una identidad gestionada asignada por el sistema.
- Opción 2: Proporcione a BlueXP las credenciales de una entidad de servicio de Azure que tenga los permisos necesarios.

Sigue estos pasos para configurar permisos para BlueXP.

Función personalizada

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

Pasos

1. Si tiene pensado instalar manualmente el software en su propio host, habilite una identidad gestionada asignada por el sistema en la máquina virtual para poder ofrecer los permisos de Azure necesarios a través de un rol personalizado.

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

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

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

   ejemplo

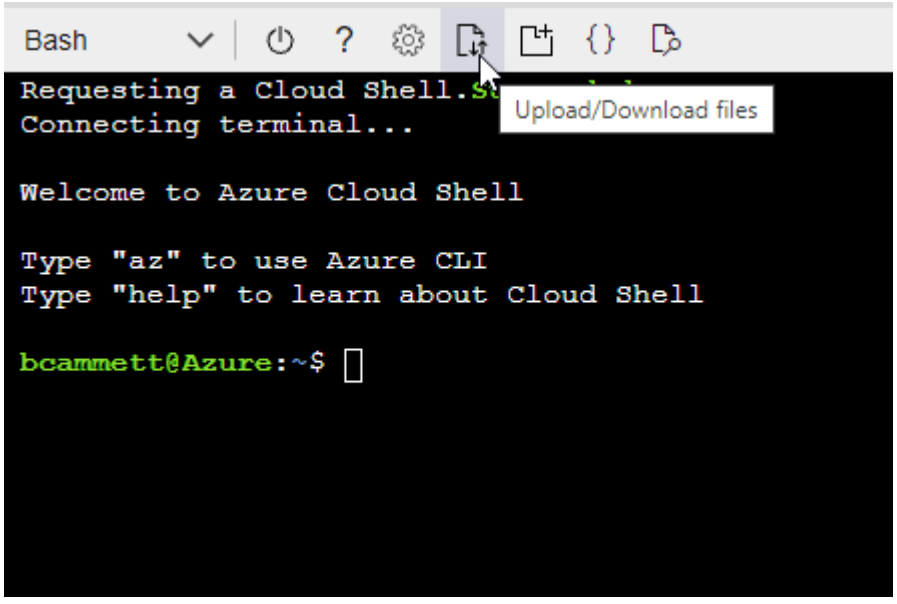
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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

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

   a. Comenzar "Shell de cloud de Azure" Y seleccione el entorno Bash.

   b. Cargue el archivo JSON.



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

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

Resultado

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

Director de servicios

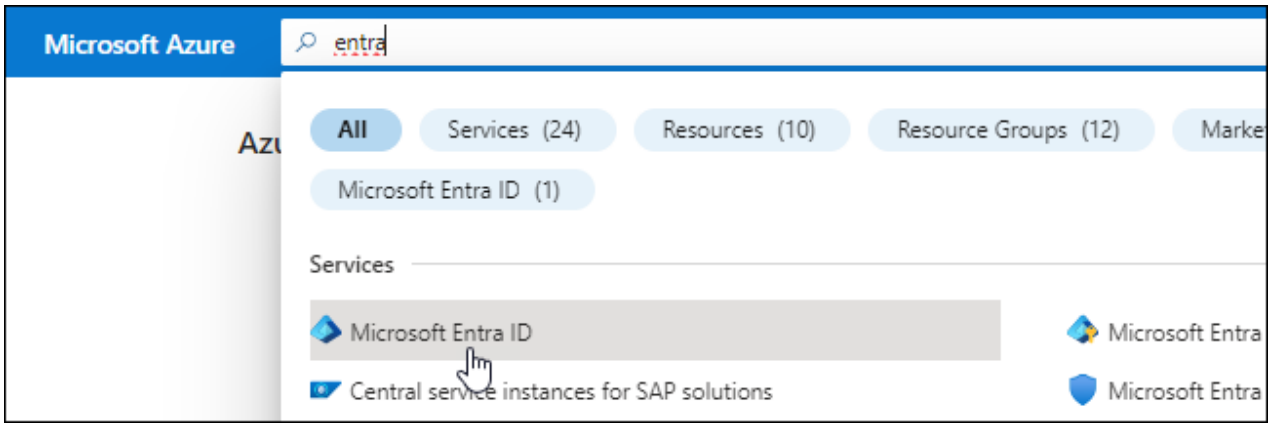
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

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

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

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

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



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

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la

CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

a. Copie el contenido de "Permisos de función personalizada para el conector" Y guárdelos en un archivo JSON.

b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

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

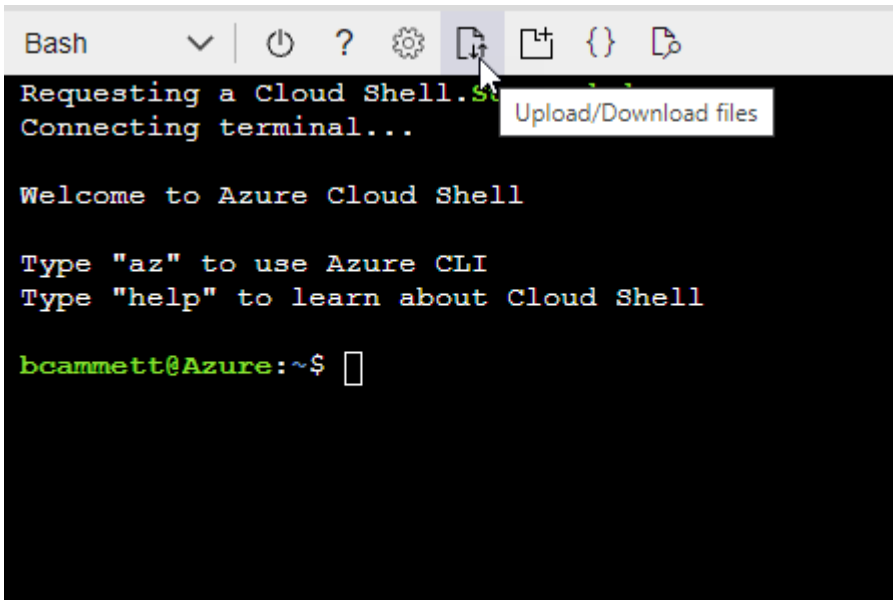
   ejemplo

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

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

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

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



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

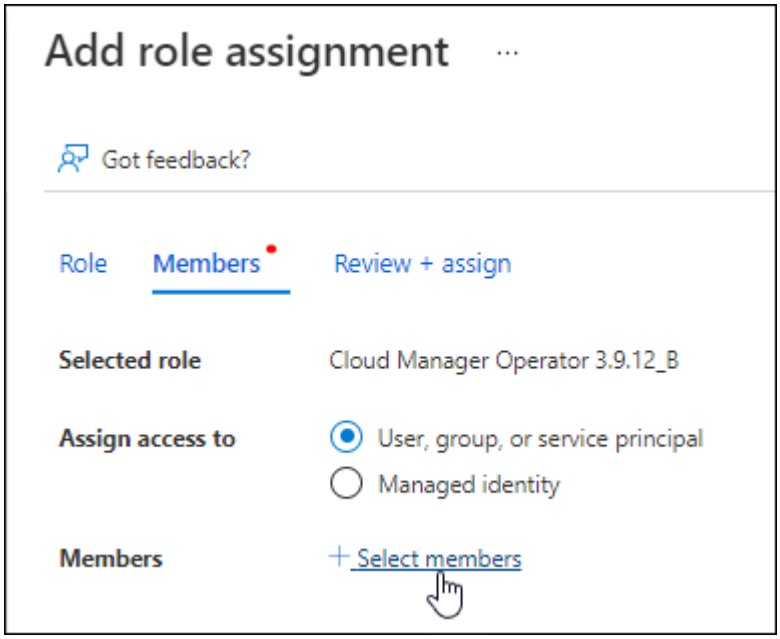
```
az role definition create --role-definition
Connector_Policy.json
```

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

2. Asigne la aplicación al rol:

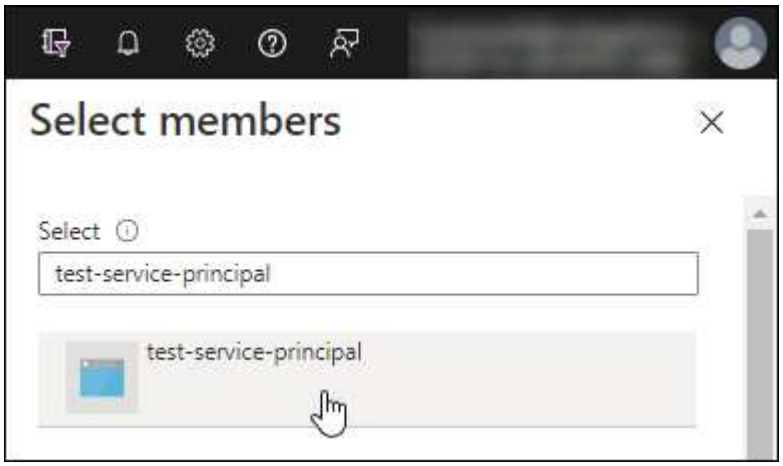
   a. En el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.
   e. En la ficha **Miembros**,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

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



      - Busque el nombre de la aplicación.

        Veamos un ejemplo:



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

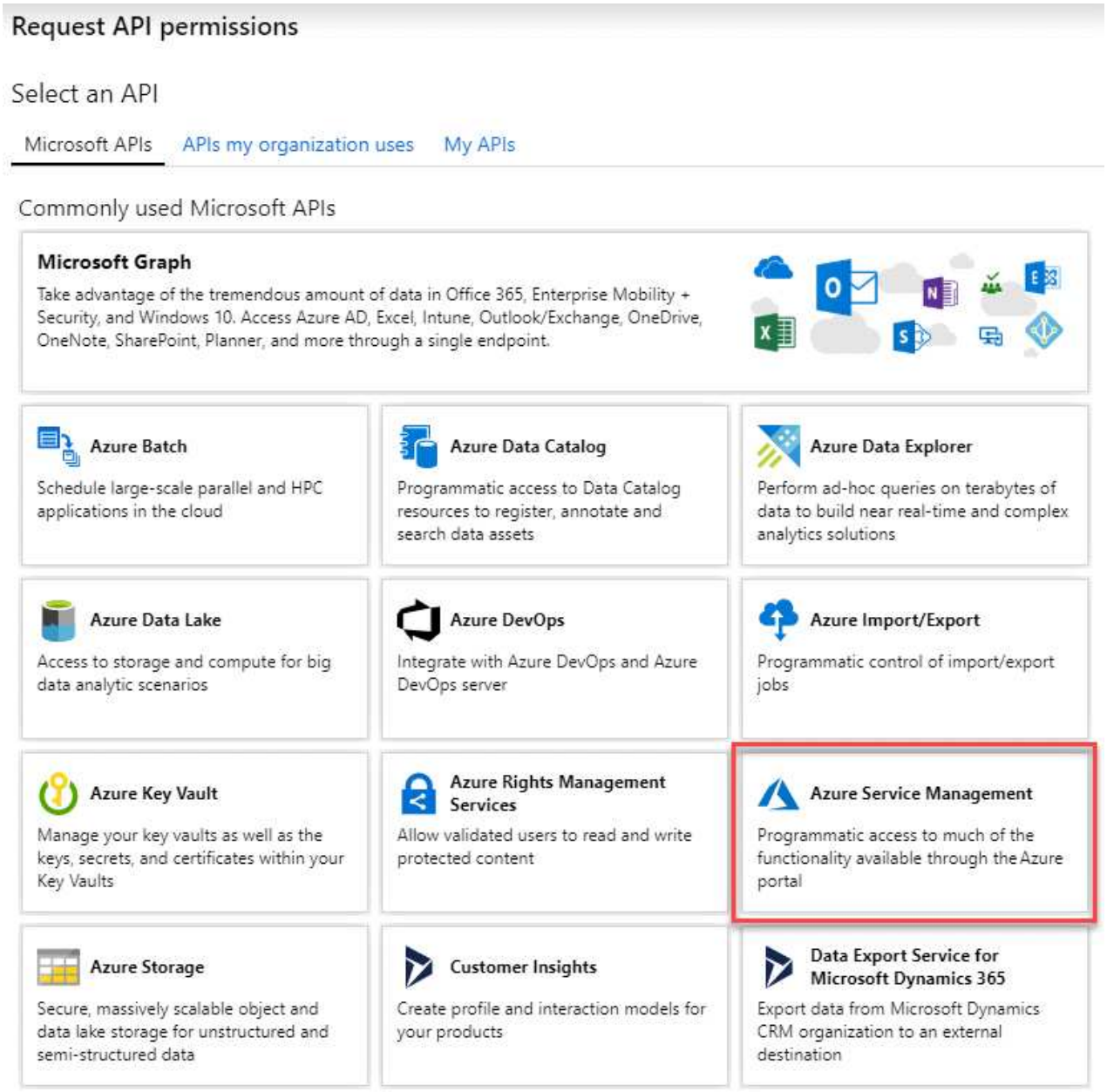
f. Seleccione **revisar + asignar**.

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

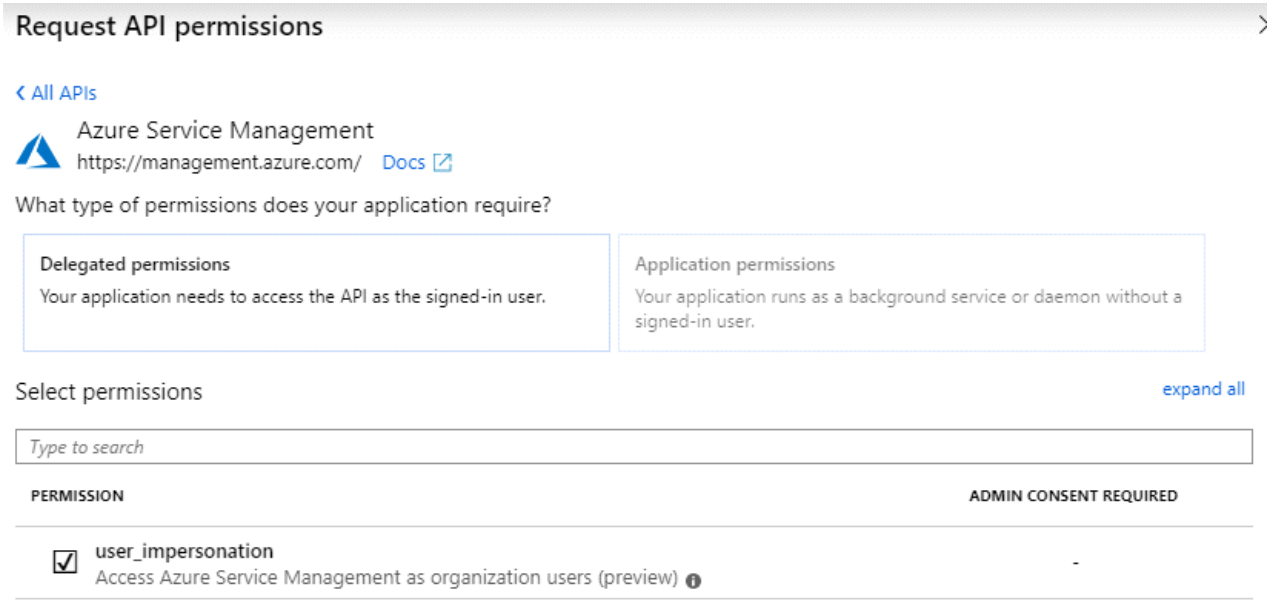
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. BlueXP le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

Añada permisos de API de administración de servicios de Windows Azure

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

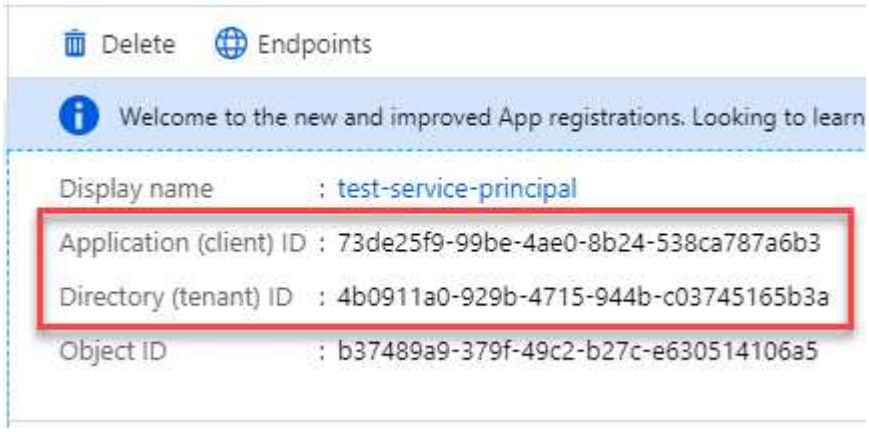


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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

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



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

Cree un secreto de cliente

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

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

Resultado

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

Paso 4: Crear el conector

Inicie Connector directamente desde Azure Marketplace.

Acerca de esta tarea

Al crear el conector desde Azure Marketplace se implementa una máquina virtual en Azure con una configuración predeterminada. "Obtenga información sobre la configuración predeterminada para el conector".

Antes de empezar

Debe tener lo siguiente:

- Una suscripción a Azure.
- Una red virtual y una subred en su región de Azure preferida.
- Detalles sobre un servidor proxy, si su empresa requiere un proxy para todo el tráfico saliente de Internet:
  - Dirección IP
  - Credenciales
  - Certificado HTTPS
- Una clave pública SSH, si desea utilizar ese método de autenticación para la máquina virtual Connector. La otra opción para el método de autenticación es usar una contraseña.

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

- Si no quiere que BlueXP cree automáticamente una función de Azure para Connector, tendrá que crear la suya propia "uso de la política en esta página".

  Estos permisos son para la propia instancia de Connector. Se trata de un conjunto de permisos diferente al configurado anteriormente para implementar la VM de Connector.

Pasos

1. Vaya a la página NetApp Connector VM del Azure Marketplace.

   "Página de Azure Marketplace para regiones comerciales"

2. Selecciona **Obtenlo ahora** y luego selecciona **Continuar**.
3. Desde el portal de Azure, seleccione **Crear** y siga los pasos para configurar la máquina virtual.

   Tenga en cuenta lo siguiente al configurar la máquina virtual:

   - **VM size**: Elija un tamaño de VM que cumpla con los requisitos de CPU y RAM. Recomendamos Standard_D8s_v3.
   - **Discos**: El conector puede funcionar de forma óptima con discos HDD o SSD.
   - **Grupo de seguridad de red**: El conector requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

     "Ver reglas de grupo de seguridad para Azure".

   - **Identidad**: En **Gestión**, seleccione **Activar identidad administrada asignada por el sistema**.

     Esta configuración es importante porque una identidad administrada permite que la máquina virtual Connector se identifique con Microsoft Entra ID sin proporcionar credenciales. "Obtenga más información sobre las identidades gestionadas para recursos de Azure".

4. En la página **Review + create**, revise sus selecciones y seleccione **Create** para iniciar la implementación.

   Azure implementa la máquina virtual con los ajustes especificados. El software de la máquina virtual y el conector debe estar funcionando en aproximadamente cinco minutos.

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

   https://ipaddress

6. Después de iniciar sesión, configure el conector:
   a. Especifique la organización BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y se configura con su organización BlueXP .

Si tienes almacenamiento de Azure Blob en la misma suscripción de Azure donde creaste el conector, verás que aparece automáticamente un entorno de trabajo de almacenamiento de Azure Blob en el lienzo de BlueXP. "Descubre cómo gestionar el almacenamiento de Azure Blob desde BlueXP"

Paso 5: Proporcionar permisos a BlueXP

Ahora que has creado Connector, debes proporcionar a BlueXP los permisos que configuraste anteriormente. Al proporcionar los permisos, BlueXP podrá gestionar sus datos y la infraestructura de almacenamiento en

Azure.

Función personalizada

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

Pasos

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

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

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

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

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

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

Resultado

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

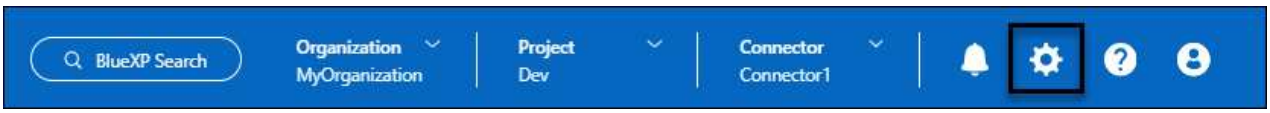
El futuro

Vaya a la "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Director de servicios

Pasos

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



2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.

a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.

b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:

   - ID de aplicación (cliente)
   - ID de directorio (inquilino)
   - Secreto de cliente

c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

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

Resultado

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

Instale manualmente el conector en Azure

Un conector es el software NetApp que se ejecuta en su red de cloud o en las instalaciones que le da la posibilidad de usar todas las funciones y servicios de BlueXP . Una de las opciones de instalación disponibles es instalar manualmente el software Connector en un host Linux que se ejecuta en Azure. Para instalar manualmente Connector en su propio host Linux, debe revisar los requisitos del host, configurar la red, preparar los permisos de Azure, instalar Connector y, a continuación, proporcionar los permisos preparados.

Antes de empezar

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

Paso 1: Revise los requisitos del host

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

Host dedicado

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

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

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

Hipervisor

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

Requisitos del sistema operativo y del contenedor

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

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Docker Engine 26.0.0	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros necesario durante la instalación del conector.

Tamaño de la máquina virtual de Azure

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

Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

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

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

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

Paso 2: Instale Podman o Docker Engine

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

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

Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 2. Pasos

Podman

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

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

Pasos

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

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

2. Instale Podman.

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

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

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

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

3. Active e inicie el servicio podman.socket.

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

4. Instale python3.

```
sudo dnf install python3
```

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

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

Para Red Hat Enterprise Linux 9:

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

Para Red Hat Enterprise Linux 8:

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

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

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

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

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

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

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 3: Configurar redes

Asegúrese de que la ubicación de red en la que planea instalar el conector admite los siguientes requisitos. Cumplir con estos requisitos permite al conector gestionar recursos y procesos dentro de tu entorno de nube híbrida.

Región de Azure

Si utiliza Cloud Volumes ONTAP, el conector debe desplegarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que gestiona, o en el "Par de regiones de Azure" Para los sistemas Cloud Volumes ONTAP. Este requisito garantiza que se utilice una conexión de enlace privado de Azure entre

Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas.

"Conozca cómo Cloud Volumes ONTAP utiliza un enlace privado de Azure"

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde los equipos cuando se utiliza la consola basada en web de BlueXP

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

"Prepare las redes para la consola de BlueXP ".

Puntos finales contactados durante la instalación manual

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

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

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

  - Los puntos finales enumerados en la opción 1 se admiten a partir de la versión 3.9.47 del conector. No hay compatibilidad con versiones anteriores del conector.
  - El conector contacta primero con los puntos finales enumerados en la opción 2. Si no se puede acceder a esos puntos finales, el conector contactará automáticamente con los puntos finales enumerados en la opción 1.

- Los extremos de la opción 1 no son compatibles si utiliza el conector con backup y recuperación de datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

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

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

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

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

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras circunstancias.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Paso 4: Configure los permisos de implementación de Connector

Necesitas proporcionar permisos de Azure a BlueXP mediante una de las siguientes opciones:

- Opción 1: Asigne un rol personalizado a la máquina virtual de Azure mediante una identidad gestionada asignada por el sistema.
- Opción 2: Proporcione a BlueXP las credenciales de una entidad de servicio de Azure que tenga los permisos necesarios.

Sigue los pasos para preparar permisos para BlueXP.

Cree un rol personalizado para el despliegue de Connector

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

Pasos

1. Si tiene pensado instalar manualmente el software en su propio host, habilite una identidad gestionada asignada por el sistema en la máquina virtual para poder ofrecer los permisos de Azure necesarios a través de un rol personalizado.

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

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

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

   ejemplo

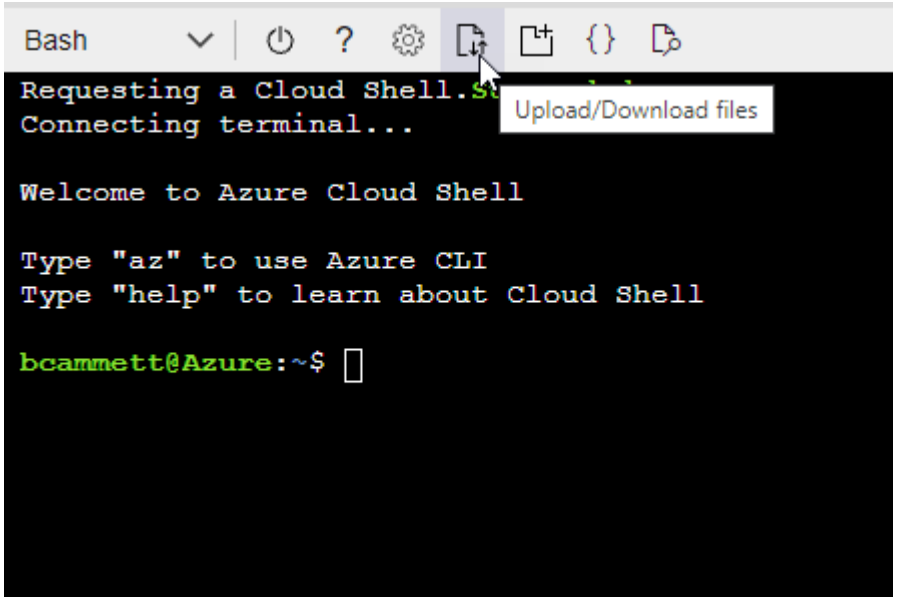
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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

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

   a. Comenzar "Shell de cloud de Azure" Y seleccione el entorno Bash.

   b. Cargue el archivo JSON.



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

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

Resultado

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

Director de servicios

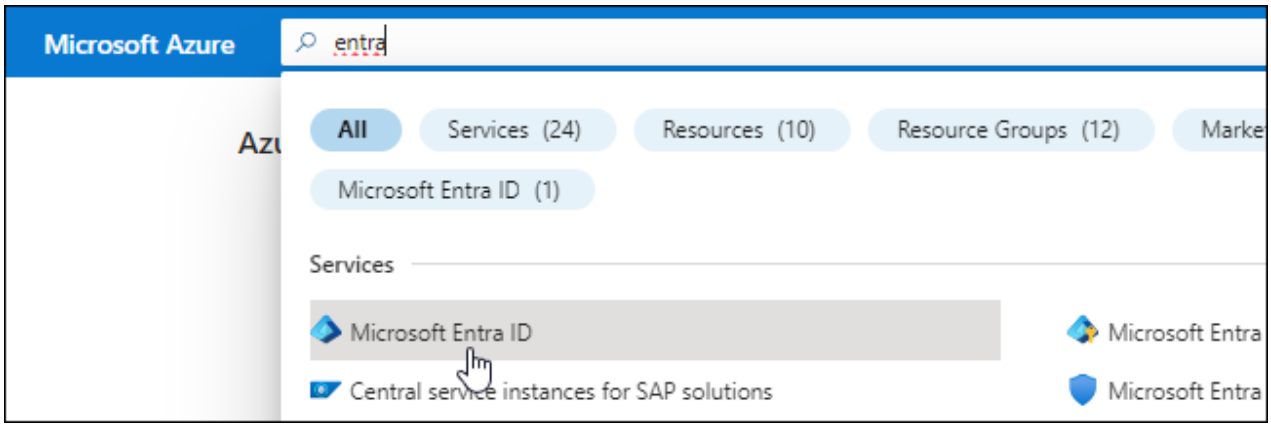
Crea y configura un director de servicio en Microsoft Entra ID y obtén las credenciales de Azure que BlueXP necesita.

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

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

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

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



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

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

   Tenga en cuenta que puede crear un rol personalizado de Azure mediante el portal de Azure, Azure PowerShell, Azure CLI o la API DE REST. Los siguientes pasos muestran cómo crear el rol con la

CLI de Azure. Si prefiere utilizar un método diferente, consulte "Documentación de Azure"

a. Copie el contenido de "Permisos de función personalizada para el conector" Y guárdelos en un archivo JSON.

b. Modifique el archivo JSON agregando ID de suscripción de Azure al ámbito asignable.

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

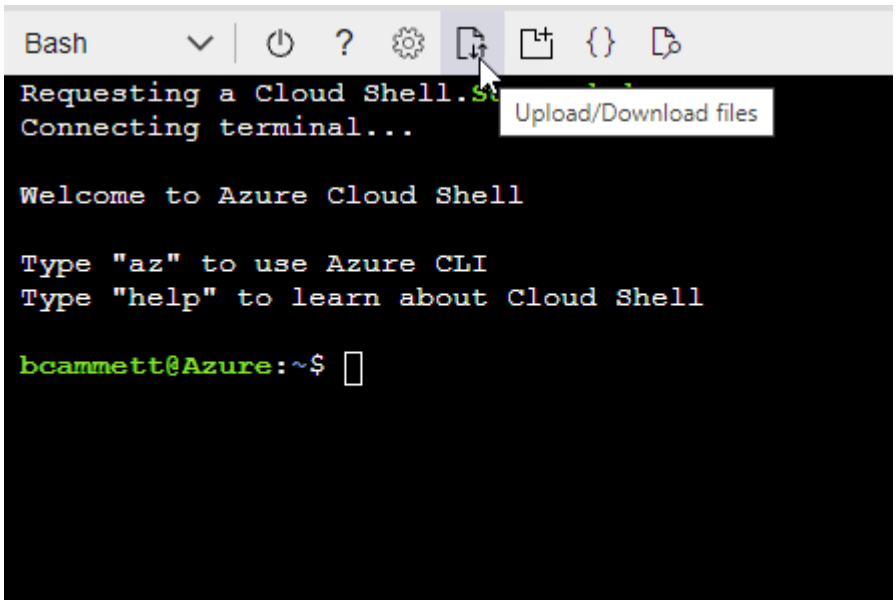
   ejemplo

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

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

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

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



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

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

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

2. Asigne la aplicación al rol:

   a. En el portal de Azure, abra el servicio **Suscripciones**.

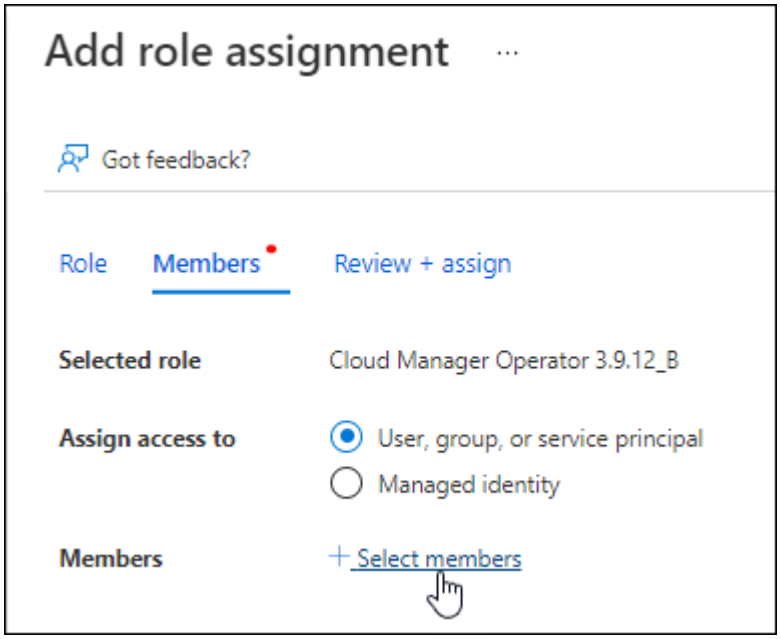
   b. Seleccione la suscripción.

   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.

   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.

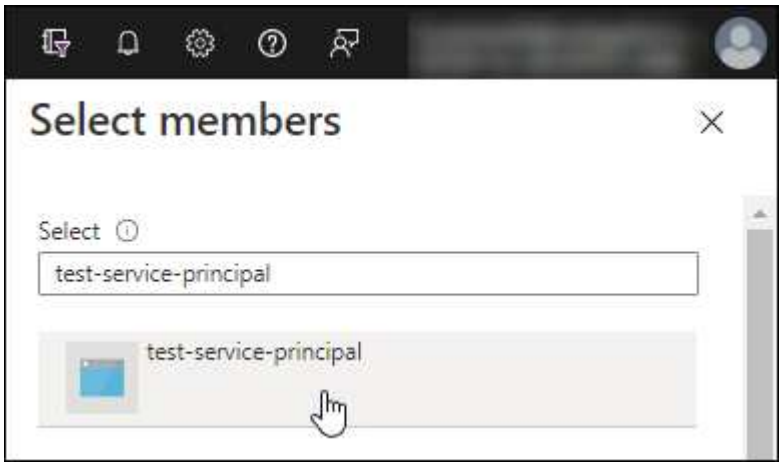
   e. En la ficha **Miembros**, realice los siguientes pasos:

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



      - Busque el nombre de la aplicación.

        Veamos un ejemplo:



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

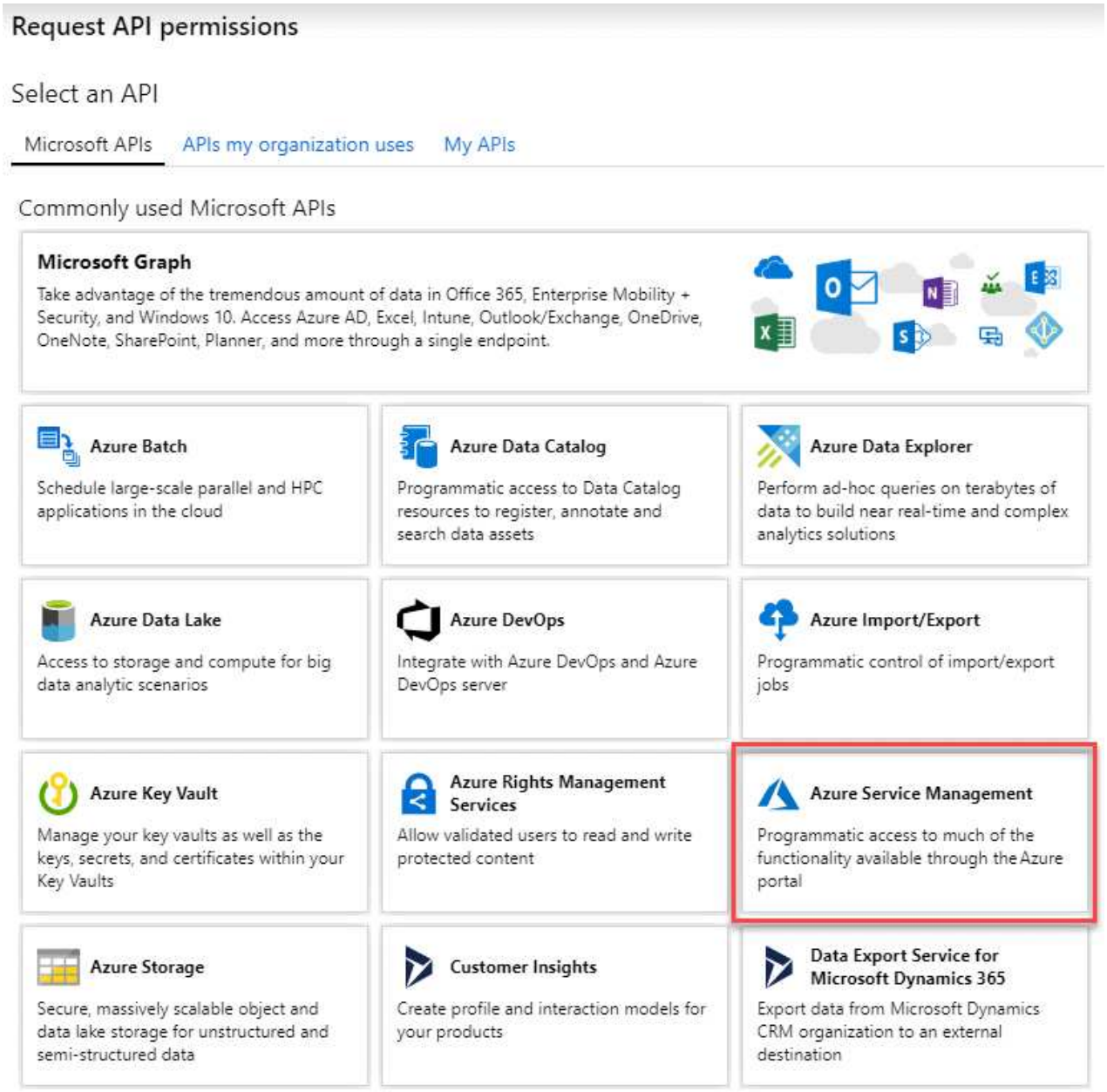
f. Seleccione **revisar + asignar**.

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

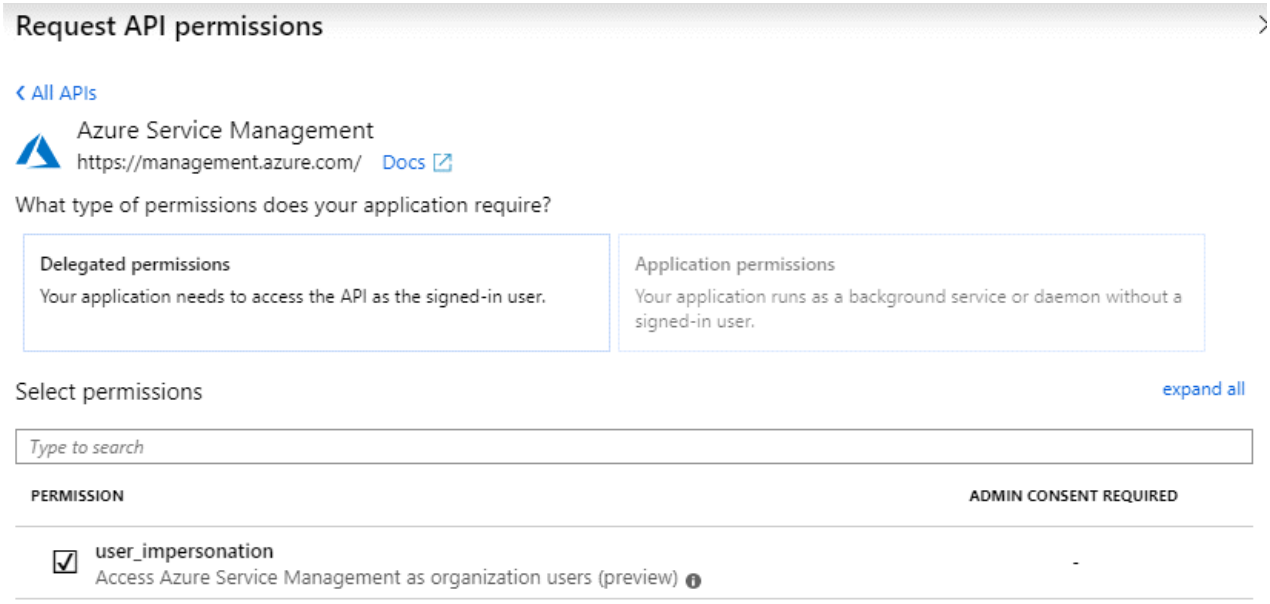
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones a Azure, debe enlazar el principal del servicio con cada una de ellas. BlueXP le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

Añada permisos de API de administración de servicios de Windows Azure

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

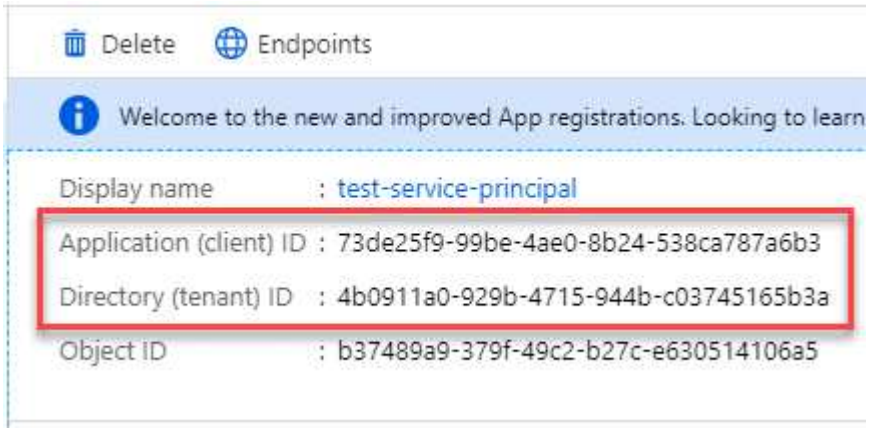


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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

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



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

Cree un secreto de cliente

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

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

Resultado

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

Paso 5: Instale el conector

Una vez completados los requisitos previos, puede instalar manualmente el software en su propio host Linux.

Antes de empezar

Debe tener lo siguiente:

- Privilegios de root para instalar el conector.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector.

  Tiene la opción de configurar un servidor proxy después de la instalación, pero para hacerlo es necesario reiniciar el conector.

  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.
- Una identidad gestionada habilitada en la máquina virtual de Azure para poder proporcionar los permisos de Azure necesarios a través de un rol personalizado.

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

Acerca de esta tarea

El instalador disponible en el sitio de soporte de NetApp puede ser una versión anterior. Después de la instalación, el conector se actualiza automáticamente si hay una nueva versión disponible.

Pasos

1. Si las variables del sistema *http_proxy* o *https_proxy* están establecidas en el host, elimínelas:

```
unset http_proxy
unset https_proxy
```

Si no elimina estas variables del sistema, la instalación fallará.

2. Descargue el software del conector de "Sitio de soporte de NetApp"Y, a continuación, cópielo en el host Linux.

   Debe descargar el instalador "en línea" del conector que se utiliza en su red o en la nube. Hay disponible un instalador "sin conexión" independiente para el conector, pero sólo es compatible con implementaciones en modo privado.

3. Asigne permisos para ejecutar el script.

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

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

4. Ejecute el script de instalación.

   ```
    ./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy server>
   --cacert <path and file name of a CA-signed certificate>
   ```

   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.

5. Espere a que finalice la instalación.

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

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

   https://ipaddress

7. Después de iniciar sesión, configure el conector:
   a. Especifique la organización BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y se configura con su organización BlueXP .

Si tienes almacenamiento de Azure Blob en la misma suscripción de Azure donde creaste el conector, verás que aparece automáticamente un entorno de trabajo de almacenamiento de Azure Blob en el lienzo de BlueXP. "Descubre cómo gestionar el almacenamiento de Azure Blob desde BlueXP"

Paso 6: Proporcionar permisos a BlueXP

Ahora que ha instalado Connector, debe proporcionar a BlueXP los permisos de Azure que configuró anteriormente. Al proporcionar los permisos, BlueXP podrá gestionar sus datos y la infraestructura de almacenamiento en Azure.

Función personalizada

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

Pasos

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

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

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

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

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

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

Resultado

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

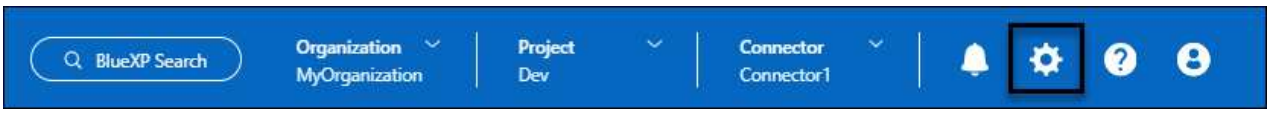
El futuro

Vaya a la "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Director de servicios

Pasos

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



2. Seleccione **Agregar Credenciales** y siga los pasos del asistente.

a. **Ubicación de credenciales**: Seleccione **Microsoft Azure > conector**.

b. **Definir Credenciales**: Introduzca información sobre el principal de servicio Microsoft Entra que otorga los permisos requeridos:

   - ID de aplicación (cliente)
   - ID de directorio (inquilino)
   - Secreto de cliente

c. **Suscripción al mercado**: Asocie una suscripción al mercado con estas credenciales suscribiendo ahora o seleccionando una suscripción existente.

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

Resultado

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

Google Cloud

Opciones de instalación del conector en Google Cloud

Hay varias formas diferentes de crear un conector en Google Cloud. Directamente desde BlueXP es la forma más común.

Están disponibles las siguientes opciones de instalación:

- "Crea el conector directamente desde BlueXP" (esta es la opción estándar)

  Esta acción inicia una instancia de máquina virtual que ejecuta Linux y el software Connector en un VPC de su elección.

- "Cree el conector con gcloud"

  Esta acción también inicia una instancia de máquina virtual que ejecuta Linux y el software Connector, pero la puesta en marcha se inicia directamente desde Google Cloud en lugar de desde BlueXP.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará a la forma en que se prepara para la instalación. Esto incluye cómo proporciona BlueXP los permisos necesarios para autenticar y administrar recursos en Google Cloud.

Crea un conector en Google Cloud desde BlueXP o gcloud

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

Antes de empezar

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

Paso 1: Configurar redes

Configure su red para que Connector pueda gestionar recursos y procesos en su entorno de cloud híbrido. Por ejemplo, debe asegurarse de que las conexiones estén disponibles para las redes de destino y de que el acceso a Internet de salida esté disponible.

VPC y subred

Al crear el conector, es necesario especificar el VPC y la subred donde debería residir el conector.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Para gestionar recursos en Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.

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

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

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

Extremos en los que se han contactado desde la consola de BlueXP

A medida que utiliza la consola basada en Web BlueXP que se proporciona a través de la capa SaaS, se pone en contacto con varios extremos para completar las tareas de gestión de datos. Esto incluye los extremos que se ponen en contacto para poner en marcha el conector desde la consola de BlueXP.

"Consulte la lista de extremos con los que se ha contactado desde la consola de BlueXP".

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras

circunstancias.

- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Deberá implementar este requisito de red después de crear el conector.

Paso 2: Configure permisos para crear el conector

Antes de poder implementar un conector desde BlueXP o mediante gcloud, debes configurar permisos para el usuario de Google Cloud que implementará la máquina virtual de Connector.

Pasos

1. Cree un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya los siguientes permisos:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
```

```
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

b. Desde Google Cloud, active Cloud Shell.

c. Cargue el archivo YAML que incluya los permisos necesarios.

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

En el ejemplo siguiente se crea un rol denominado "connectorDeployment" en el nivel de proyecto:

Los roles de gcloud iam crean connectorDeployment --project=myproject --file=Connector -deployment.yaml

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

2. Asigne esta función personalizada al usuario que implementará Connector desde BlueXP o mediante gcloud.

"Google Cloud docs: Conceda un único rol"

Resultado

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

Paso 3: Configurar permisos para el conector

Se necesita una cuenta de servicio de Google Cloud para proporcionar al Connector los permisos que BlueXP necesita para gestionar recursos en Google Cloud. Cuando cree el Connector, deberá asociar esta cuenta de servicio con la VM de Connector.

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

Pasos

1. Cree un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya el contenido de "Permisos de cuenta de servicio para el conector".
   b. Desde Google Cloud, active Cloud Shell.
   c. Cargue el archivo YAML que incluya los permisos necesarios.
   d. Cree un rol personalizado mediante `gcloud iam roles create` comando.

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

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

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

2. Cree una cuenta de servicio en Google Cloud y asígnele el rol a la cuenta de servicio:

   a. En el servicio IAM y Admin, selecciona **Cuentas de servicio > Crear cuenta de servicio**.
   b. Ingrese los detalles de la cuenta de servicio y seleccione **Crear y continuar**.
   c. Seleccione la función que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

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

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

   Por ejemplo, supongamos que el conector está en el proyecto 1 y que desea crear sistemas Cloud

Volumes ONTAP en el proyecto 2. Tendrá que otorgar acceso a la cuenta de servicio en el proyecto 2.

a. En el servicio IAM & Admin, seleccione el proyecto de Google Cloud en el que desea crear sistemas Cloud Volumes ONTAP.
b. En la página **IAM**, seleccione **conceder acceso** y proporcione la información necesaria.
   - Introduzca el correo electrónico de la cuenta de servicio del conector.
   - Seleccione el rol personalizado del conector.
   - Seleccione **Guardar**.

Para obtener información detallada, consulte "Documentación de Google Cloud"

Resultado

Se ha configurado la cuenta de servicio del conector VM.

Paso 4: Configurar permisos de VPC compartidos

Si utiliza un VPC compartido para implementar recursos en un proyecto de servicio, tendrá que preparar los permisos.

Esta tabla es de referencia y el entorno debe reflejar la tabla de permisos cuando se haya completado la configuración de IAM.

Ver permisos de VPC compartidos

Identidad	Creador	Alojadas en	Permisos de proyecto de servicio	Permisos del proyecto host	Específico
Cuenta de Google para desplegar el conector	Personalizado	Proyecto de servicio	"Política de despliegue de conectores"	compute.networkUser	Despliegue del conector en el proyecto de servicio
Cuenta de servicio del conector	Personalizado	Proyecto de servicio	"Política de cuenta de servicio de conector"	compute.networkUser deploymentmanager.editor	Implementación y mantenimiento de Cloud Volumes ONTAP y servicios en el proyecto de servicio
Cuenta de servicio de Cloud Volumes ONTAP	Personalizado	Proyecto de servicio	storage.admin miembro: Cuenta de servicio de BlueXP como serviceAccount.user	N.A.	(Opcional) para la organización de datos en niveles y el backup y recuperación de BlueXP
Agente de servicio de API de Google	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	compute.networkUser	Interactúa con las API de Google Cloud en nombre de la implementación. Permite a BlueXP utilizar la red compartida.
Cuenta de servicio predeterminada de Google Compute Engine	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	compute.networkUser	Pone en marcha instancias de Google Cloud e infraestructura de computación en nombre de la puesta en marcha. Permite a BlueXP utilizar la red compartida.

Notas:

1. deploymentmanager.editor sólo es necesario en el proyecto host si no pasa reglas de firewall a la implementación y decide dejar que BlueXP las cree por usted. BlueXP creará una implementación en el proyecto host que contiene la regla de firewall VPC0 si no se especifica ninguna regla.
2. Firewall.create y firewall.delete sólo son necesarios si no está pasando reglas de firewall a la implementación y está eligiendo permitir que BlueXP las cree para usted. Estos permisos residen en el archivo .yaml de cuenta de BlueXP. Si va a implementar un par de alta disponibilidad mediante un VPC compartido, estos permisos se utilizarán para crear las reglas de firewall para VPC1, 2 y 3. Para todas las demás implementaciones, estos permisos también se utilizarán para crear reglas para

VPC0.

3. Para la organización en niveles de los datos, la cuenta del servicio de organización en niveles debe tener el rol serviceAccount.user en la cuenta de servicio, no solo en el nivel del proyecto. Actualmente, si asigna serviceAccount.user en el nivel de proyecto, los permisos no se muestran cuando consulta la cuenta de servicio con getIAMPolicy.

Paso 5: Habilita las API de Google Cloud

Se deben habilitar varias API de Google Cloud antes de poder implementar Connector y Cloud Volumes ONTAP en Google Cloud.

Paso

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

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

"Documentación de Google Cloud: Habilitar API"

Paso 6: Crear el conector

Crea un conector directamente desde la consola web de BlueXP o mediante gcloud.

Acerca de esta tarea

La creación de Connector implementa una instancia de máquina virtual en Google Cloud mediante una configuración predeterminada. Después de crear el conector, no debe cambiar a una instancia de VM más pequeña que tenga menos CPU o RAM. "Obtenga información sobre la configuración predeterminada para el conector".

BlueXP

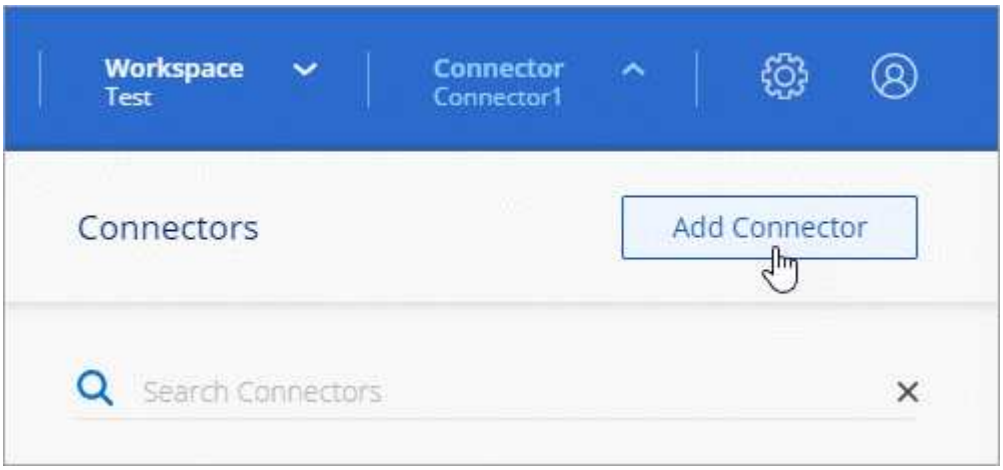
Antes de empezar

Debe tener lo siguiente:

- Los permisos necesarios de Google Cloud para crear el conector y una cuenta de servicio para el conector VM.
- Un VPC y una subred que cumplan los requisitos de red.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector.

Pasos

1. Seleccione la lista desplegable **Connector** y seleccione **Add Connector**.



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

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

   - **Detalles**: Introduzca un nombre para la instancia de la máquina virtual, especifique etiquetas, seleccione un proyecto y, a continuación, seleccione la cuenta de servicio que tenga los permisos necesarios (consulte la sección anterior para obtener más información).
   - **ubicación**: Especifique una región, zona, VPC y subred para la instancia.
   - **Red**: Elija si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
   - **Política de firewall**: Elija si desea crear una nueva política de firewall o si desea seleccionar una política de firewall existente que permita las reglas de entrada y salida requeridas.

"Reglas de firewall en Google Cloud"

- **Revisión**: Revise sus selecciones para verificar que su configuración es correcta.

5. Seleccione **Agregar**.

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

Resultado

Una vez completado el proceso, el conector está disponible para su uso en BlueXP.

Si tienes buckets de Google Cloud Storage en la misma cuenta de Google Cloud en la que creaste el conector, verás que el entorno de trabajo de Google Cloud Storage aparece automáticamente en el lienzo de BlueXP. "Descubre cómo gestionar Google Cloud Storage desde BlueXP"

gcloud

Antes de empezar

Debe tener lo siguiente:

- Los permisos necesarios de Google Cloud para crear el conector y una cuenta de servicio para el conector VM.
- Un VPC y una subred que cumplan los requisitos de red.
- Comprensión de los requisitos de instancia de VM.
  - **CPU**: 8 núcleos o 8 vCPU
  - **RAM**: 32 GB
  - * Tipo de máquina *: Recomendamos n2-standard-8.

    El conector es compatible con Google Cloud en una instancia de VM con un SO que admite las características de VM blindadas.

Pasos

1. Inicie sesión en el SDK de gcloud 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-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

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

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

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

zona
: La zona en la que desea implementar la máquina virtual

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

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

ruta de la red

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

ruta de subred

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

km-clave-ruta

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

Para obtener más información acerca de estas marcas, visite "Documentación sobre Google Cloud Computing SDK".

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

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

   https://ipaddress

2. Después de iniciar sesión, configure el conector:
   a. Especifique la organización BlueXP que desea asociar al conector.

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

   b. Escriba un nombre para el sistema.

Resultado

El conector ya está instalado y configurado con su organización BlueXP .

Abra un explorador web y vaya al "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Instale manualmente el conector en Google Cloud

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

Antes de empezar

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

Paso 1: Revise los requisitos del host

El software del conector debe ejecutarse en un host que cumpla con requisitos específicos del sistema

operativo, requisitos de RAM, requisitos de puerto, etc.

Host dedicado

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

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

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

Hipervisor

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

Requisitos del sistema operativo y del contenedor

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

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Docker Engine 26.0.0	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros necesario durante la instalación del conector.

Tipo de máquina de Google Cloud

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

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

Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

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

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

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

Paso 2: Instale Podman o Docker Engine

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

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

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 3. Pasos

Podman

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

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

Pasos

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

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

2. Instale Podman.

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

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

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

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

3. Active e inicie el servicio podman.socket.

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

4. Instale python3.

```
sudo dnf install python3
```

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

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

Para Red Hat Enterprise Linux 9:

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

Para Red Hat Enterprise Linux 8:

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

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

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

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

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

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

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 3: Configurar redes

Configure su red para que Connector pueda gestionar recursos y procesos en su entorno de cloud híbrido. Por ejemplo, debe asegurarse de que las conexiones estén disponibles para las redes de destino y de que el acceso a Internet de salida esté disponible.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde los equipos cuando se utiliza la consola basada en web de BlueXP

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

"Prepare las redes para la consola de BlueXP ".

Puntos finales contactados durante la instalación manual

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

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

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

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

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

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Para gestionar recursos en Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendado) [1] https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para actualizaciones de Connector.

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

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

datos de BlueXP o la protección contra ransomware de BlueXP . En este caso, puede desactivar los puntos finales enumerados en la opción 1, mientras permite los puntos finales enumerados en la opción 2.

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras circunstancias.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Paso 4: Configurar permisos para el conector

Se necesita una cuenta de servicio de Google Cloud para proporcionar al Connector los permisos que BlueXP necesita para gestionar recursos en Google Cloud. Cuando cree el Connector, deberá asociar esta cuenta de servicio con la VM de Connector.

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

Pasos

1. Cree un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya el contenido de "Permisos de cuenta de servicio para el conector".

   b. Desde Google Cloud, active Cloud Shell.

   c. Cargue el archivo YAML que incluya los permisos necesarios.

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

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

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

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

2. Cree una cuenta de servicio en Google Cloud y asígnele el rol a la cuenta de servicio:
   a. En el servicio IAM y Admin, selecciona **Cuentas de servicio > Crear cuenta de servicio**.
   b. Ingrese los detalles de la cuenta de servicio y seleccione **Crear y continuar**.
   c. Seleccione la función que acaba de crear.
   d. Finalice los pasos restantes para crear la función.

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

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

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

   a. En el servicio IAM & Admin, seleccione el proyecto de Google Cloud en el que desea crear sistemas Cloud Volumes ONTAP.
   b. En la página **IAM**, seleccione **conceder acceso** y proporcione la información necesaria.
      - Introduzca el correo electrónico de la cuenta de servicio del conector.
      - Seleccione el rol personalizado del conector.
      - Seleccione **Guardar**.

   Para obtener información detallada, consulte "Documentación de Google Cloud"

Resultado

Se ha configurado la cuenta de servicio del conector VM.

Paso 5: Configurar permisos de VPC compartidos

Si utiliza un VPC compartido para implementar recursos en un proyecto de servicio, tendrá que preparar los permisos.

Esta tabla es de referencia y el entorno debe reflejar la tabla de permisos cuando se haya completado la configuración de IAM.

Ver permisos de VPC compartidos

Identidad	Creador	Alojadas en	Permisos de proyecto de servicio	Permisos del proyecto host	Específico
Cuenta de Google para desplegar el conector	Personalizado	Proyecto de servicio	"Política de despliegue de conectores"	compute.networkUser	Despliegue del conector en el proyecto de servicio
Cuenta de servicio del conector	Personalizado	Proyecto de servicio	"Política de cuenta de servicio de conector"	compute.networkUser deploymentmanager.editor	Implementación y mantenimiento de Cloud Volumes ONTAP y servicios en el proyecto de servicio
Cuenta de servicio de Cloud Volumes ONTAP	Personalizado	Proyecto de servicio	storage.admin miembro: Cuenta de servicio de BlueXP como serviceAccount.user	N.A.	(Opcional) para la organización de datos en niveles y el backup y recuperación de BlueXP
Agente de servicio de API de Google	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	compute.networkUser	Interactúa con las API de Google Cloud en nombre de la implementación. Permite a BlueXP utilizar la red compartida.
Cuenta de servicio predeterminada de Google Compute Engine	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	compute.networkUser	Pone en marcha instancias de Google Cloud e infraestructura de computación en nombre de la puesta en marcha. Permite a BlueXP utilizar la red compartida.

Notas:

1. deploymentmanager.editor sólo es necesario en el proyecto host si no pasa reglas de firewall a la implementación y decide dejar que BlueXP las cree por usted. BlueXP creará una implementación en el proyecto host que contiene la regla de firewall VPC0 si no se especifica ninguna regla.
2. Firewall.create y firewall.delete sólo son necesarios si no está pasando reglas de firewall a la implementación y está eligiendo permitir que BlueXP las cree para usted. Estos permisos residen en el archivo .yaml de cuenta de BlueXP. Si va a implementar un par de alta disponibilidad mediante un VPC compartido, estos permisos se utilizarán para crear las reglas de firewall para VPC1, 2 y 3. Para todas las demás implementaciones, estos permisos también se utilizarán para crear reglas para

VPC0.

3. Para la organización en niveles de los datos, la cuenta del servicio de organización en niveles debe tener el rol serviceAccount.user en la cuenta de servicio, no solo en el nivel del proyecto. Actualmente, si asigna serviceAccount.user en el nivel de proyecto, los permisos no se muestran cuando consulta la cuenta de servicio con getIAMPolicy.

Paso 6: Habilita las API de Google Cloud

Se deben habilitar varias API de Google Cloud antes de poder implementar sistemas de Cloud Volumes ONTAP en Google Cloud.

Paso

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

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

"Documentación de Google Cloud: Habilitar API"

Paso 7: Instale el conector

Una vez completados los requisitos previos, puede instalar manualmente el software en su propio host Linux.

Antes de empezar

Debe tener lo siguiente:

- Privilegios de root para instalar el conector.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector.

  Tiene la opción de configurar un servidor proxy después de la instalación, pero para hacerlo es necesario reiniciar el conector.

  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.

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.

5. Espere a que finalice la instalación.

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

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

   https://ipaddress

7. Después de iniciar sesión, configure el conector:
   a. Especifique la organización BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. Sólo debe activar el modo restringido si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de entorno de administración de BlueXP. Si ese es el caso, "Siga los pasos para comenzar con BlueXP en modo restringido".

   d. Selecciona **Comenzar**.

Resultado

El conector ya está instalado y se configura con su organización BlueXP .

Si tienes buckets de Google Cloud Storage en la misma cuenta de Google Cloud en la que creaste el conector, verás que el entorno de trabajo de Google Cloud Storage aparece automáticamente en el lienzo de BlueXP. "Descubre cómo gestionar Google Cloud Storage desde BlueXP"

Paso 8: Proporcionar permisos a BlueXP

Tienes que proporcionar a BlueXP los permisos de Google Cloud que hayas configurado anteriormente. Al proporcionar los permisos, BlueXP podrá gestionar tus datos y la infraestructura de almacenamiento en Google Cloud.

Pasos

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

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

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

Resultado

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

Instale y configure un conector en las instalaciones

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

Antes de empezar

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

Paso 1: Revise los requisitos del host

El software del conector debe ejecutarse en un host que cumpla con requisitos específicos del sistema operativo, requisitos de RAM, requisitos de puerto, etc. Asegúrese de que el host cumple estos requisitos antes de instalar el conector.

Host dedicado

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

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

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

Hipervisor

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

Requisitos del sistema operativo y del contenedor

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

De NetApp	Versiones de OS compatibles	Versiones de conector admitidas	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux	9,1 a 9,4 8,6 a 8,10 7,9	3.9.40 o posterior con BlueXP en modo estándar o restringido	Podman versión 4.6.1 o 4.9.4 Ver los requisitos de configuración de Podman.	Compatible con el modo de aplicación o el modo permisivo [1]
Ubuntu	24,04 LTS	3.9.45 o posterior con BlueXP en modo estándar o restringido	Docker Engine 26.0.0	No admitido

Notas:

1. La gestión de sistemas Cloud Volumes ONTAP no es compatible con conectores que tienen SELinux activado en el sistema operativo.
2. El conector es compatible con las versiones en inglés de estos sistemas operativos.
3. Para RHEL, el host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros necesario durante la instalación del conector.

Espacio en disco en /opt

Debe haber 100 GIB de espacio disponibles

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

Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

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

Paso 2: Instale Podman o Docker Engine

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

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

  Ver las versiones de Podman que admite BlueXP .

- Se requiere Docker Engine para Ubuntu.

  Vea las versiones de Docker Engine compatibles con BlueXP .

Ejemplo 4. Pasos

Podman

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

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

Pasos

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

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

2. Instale Podman.

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

   Para Red Hat Enterprise Linux 9:

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

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

   Para Red Hat Enterprise Linux 8:

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

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

3. Active e inicie el servicio podman.socket.

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

4. Instale python3.

```
sudo dnf install python3
```

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

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

Para Red Hat Enterprise Linux 9:

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

Para Red Hat Enterprise Linux 8:

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

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

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

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

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Consulte las instrucciones de instalación de Docker"

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

2. Compruebe que Docker está habilitado y en ejecución.

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

Paso 3: Configurar redes

Configure su red para que Connector pueda gestionar recursos y procesos en su entorno de cloud híbrido. Por ejemplo, debe asegurarse de que las conexiones estén disponibles para las redes de destino y de que el acceso a Internet de salida esté disponible.

Conexiones a redes de destino

Un conector requiere una conexión de red a la ubicación en la que tiene previsto crear y administrar entornos de trabajo. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red en la que se despliega el conector debe tener una conexión a Internet saliente para contactar con puntos finales específicos.

Puntos finales contactados desde los equipos cuando se utiliza la consola basada en web de BlueXP

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

"Prepare las redes para la consola de BlueXP ".

Puntos finales contactados durante la instalación manual

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

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

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

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

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

Puntos finales contactados desde el conector

El conector requiere acceso a Internet saliente para contactar con los siguientes puntos finales con el fin de administrar los recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Tenga en cuenta que los puntos finales que se muestran a continuación son todas las entradas de CNAME.

Puntos finales	Específico
Servicios de AWS (amazonaws.com): • Formación CloudFormation • Cloud computing elástico (EC2) • Gestión de acceso e identidad (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Simple Storage Service (S3)	Para gestionar recursos en AWS. El punto final exacto depende de la región de AWS que esté utilizando. "Consulte la documentación de AWS para obtener más detalles"
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Para gestionar recursos en regiones públicas de Azure.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	Para gestionar recursos en regiones de Azure China.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	Para gestionar recursos en Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Para obtener información sobre licencias y enviar mensajes de AutoSupport al soporte de NetApp.
https://*.api.BlueXP .NetApp.com https://api.BlueXP .NetApp.com https://*.cloudmanager.cloud.NetApp.com https://cloudmanager.cloud.NetApp.com https://NetApp-cloud-account.auth0.com	Proporcionar funciones y servicios SaaS dentro de BlueXP.

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

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

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

Servidor proxy

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

- Dirección IP
- Credenciales
- Certificado HTTPS

Puertos

No hay tráfico entrante al conector, a menos que lo inicie o si el conector se utiliza como proxy para enviar mensajes de AutoSupport desde Cloud Volumes ONTAP al soporte de NetApp.

- HTTP (80) y HTTPS (443) proporcionan acceso a la interfaz de usuario local, que utilizará en raras circunstancias.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Las conexiones de entrada a través del puerto 3128 son necesarias si implementa sistemas Cloud Volumes ONTAP en una subred en la que no hay una conexión de Internet de salida disponible.

  Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar

mensajes de AutoSupport, BlueXP configura automáticamente esos sistemas para que usen un servidor proxy incluido en el conector. El único requisito es asegurarse de que el grupo de seguridad del conector permite conexiones entrantes a través del puerto 3128. Tendrá que abrir este puerto después de desplegar el conector.

Habilite NTP

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

Paso 4: Configure los permisos de la nube

Si quieres usar los servicios de BlueXP en AWS o Azure con un conector on-premises, necesitas configurar permisos en tu proveedor de nube para que puedas añadir las credenciales al conector después de instalarlo.

¿Por qué no Google Cloud? Cuando Connector está instalado en las instalaciones, no puede gestionar sus recursos en Google Cloud. El conector debe estar instalado en Google Cloud para administrar los recursos que residen allí.

AWS

Cuando el conector se instala en las instalaciones, debe proporcionar a BlueXP permisos de AWS agregando claves de acceso para un usuario de IAM que tenga los permisos necesarios.

Debe utilizar este método de autenticación si el conector está instalado en las instalaciones. No se puede utilizar la función IAM.

Pasos

1. Inicie sesión en la consola de AWS y desplácese al servicio IAM.
2. Cree una política:

    a. Selecciona **Políticas > Crear política**.

    b. Seleccione **JSON** y copie y pegue el contenido del "Política de IAM para el conector".

    c. Finalice los pasos restantes para crear la directiva.

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

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

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

Resultado

Ahora debe tener claves de acceso para un usuario de IAM que tenga los permisos necesarios. Después de instalar el conector, deberá asociar estas credenciales con el conector de BlueXP.

Azure

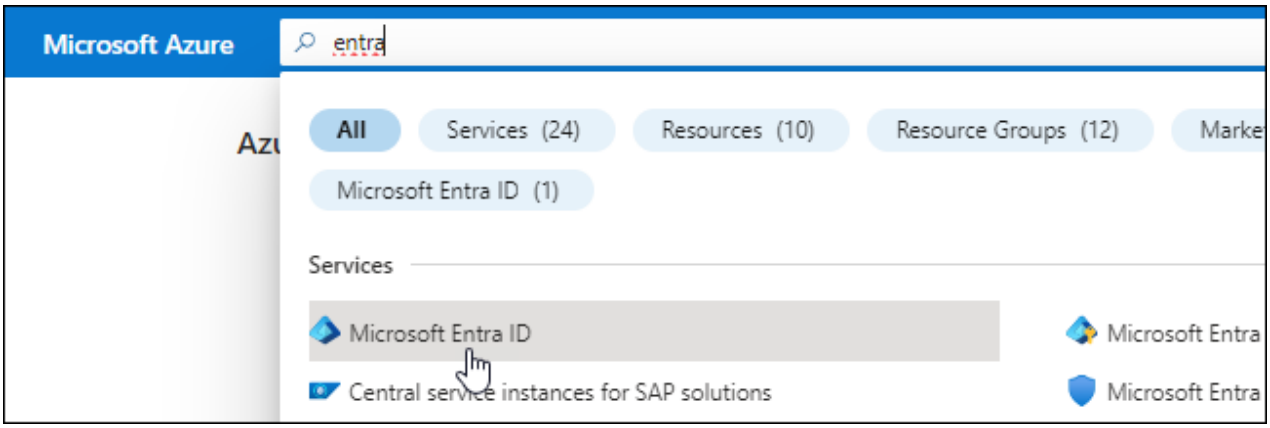
Cuando el conector se instala en las instalaciones, debe proporcionar a BlueXP permisos de Azure configurando un principal de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que BlueXP necesita.

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

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

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

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



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

   Ha creado la aplicación AD y el director de servicio.

Asigne la aplicación a una función

1. Crear un rol personalizado:

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

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

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

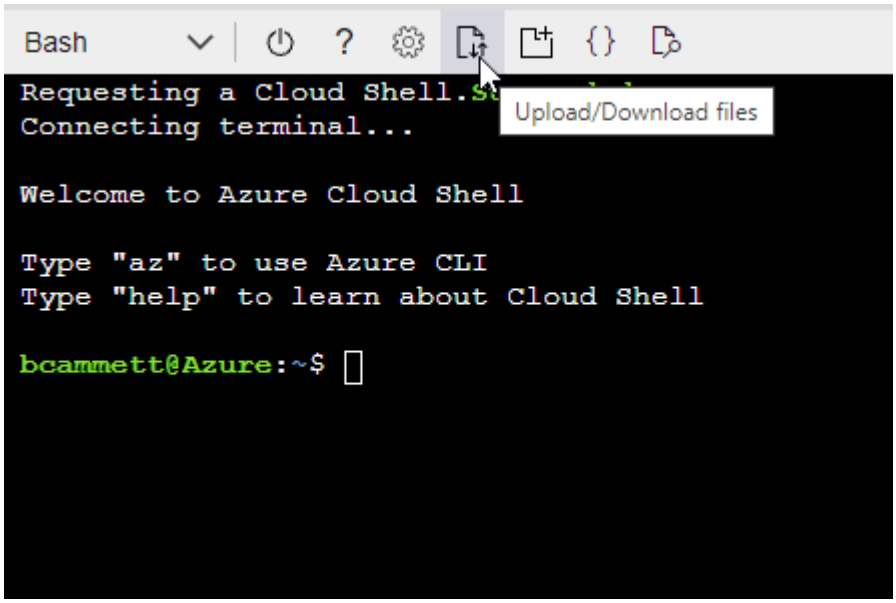
      ejemplo

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

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

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

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



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

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

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

2. Asigne la aplicación al rol:

   a. En el portal de Azure, abra el servicio **Suscripciones**.

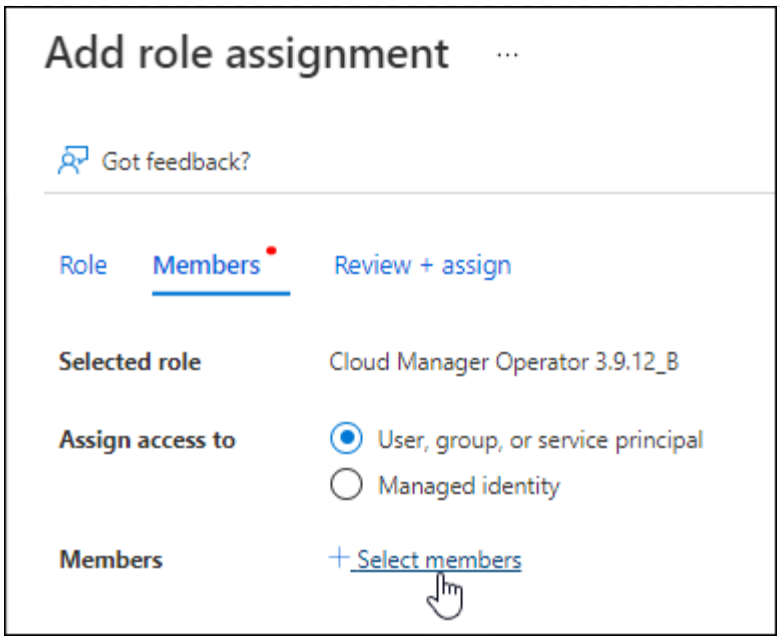
   b. Seleccione la suscripción.

   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.

   d. En la ficha **rol**, seleccione el rol **operador de BlueXP** y seleccione **Siguiente**.

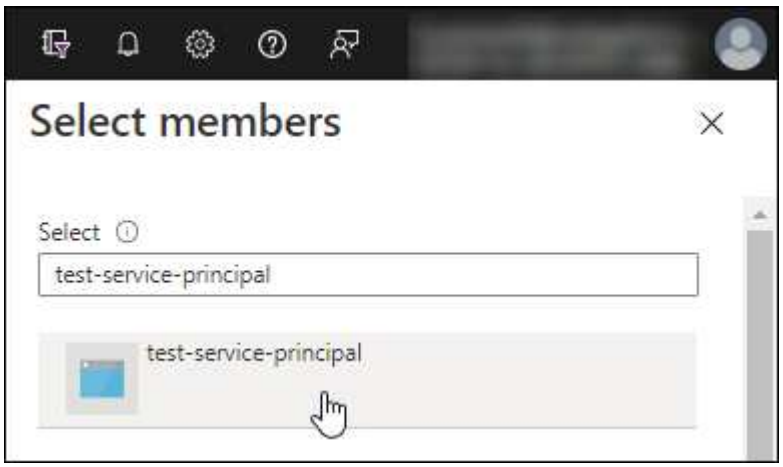
   e. En la ficha **Miembros**, realice los siguientes pasos:

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



- Busque el nombre de la aplicación.

  Veamos un ejemplo:



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

f. Seleccione **revisar + asignar**.

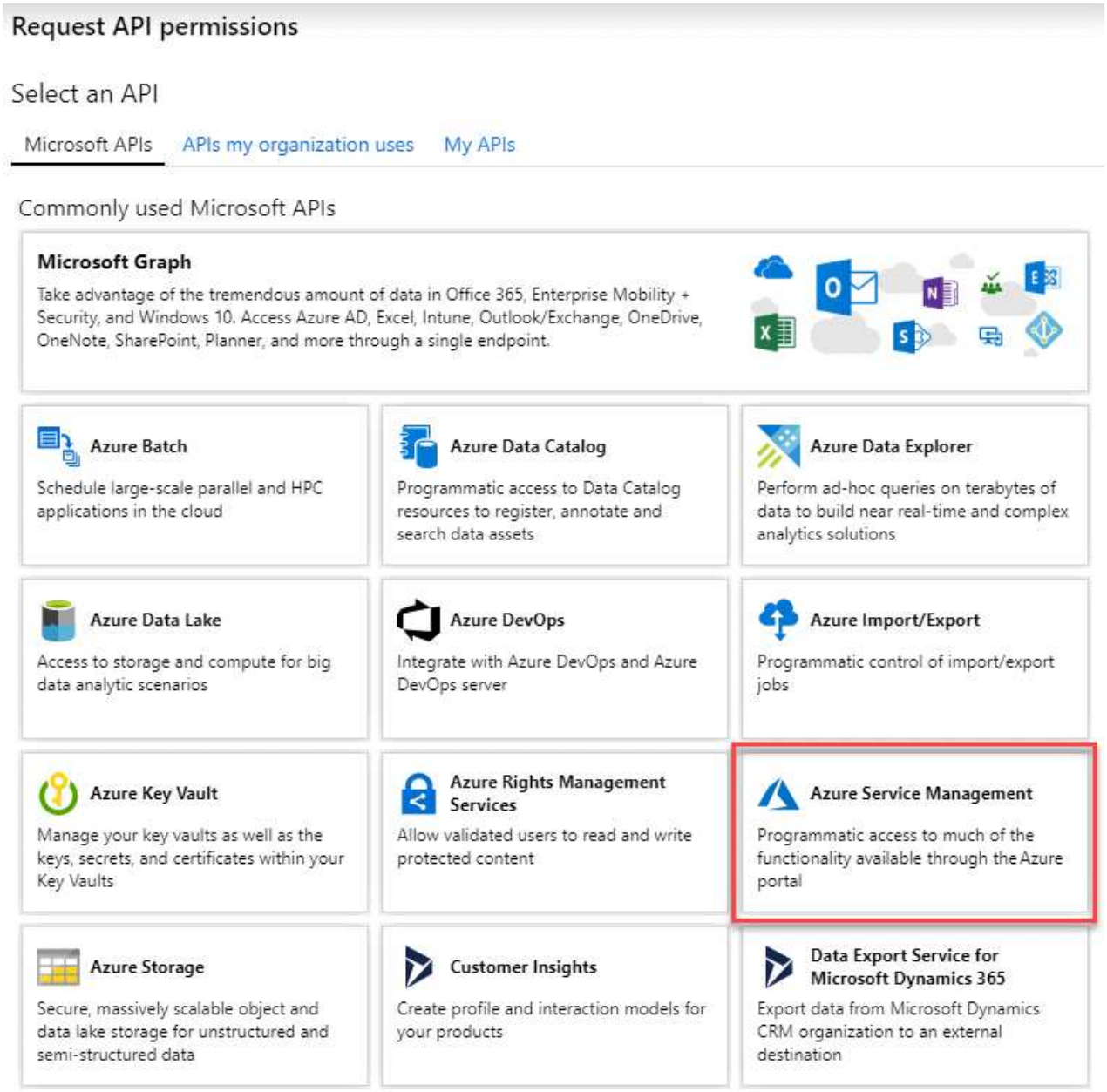
El principal de servicio ahora tiene los permisos de Azure necesarios para implementar el conector.

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

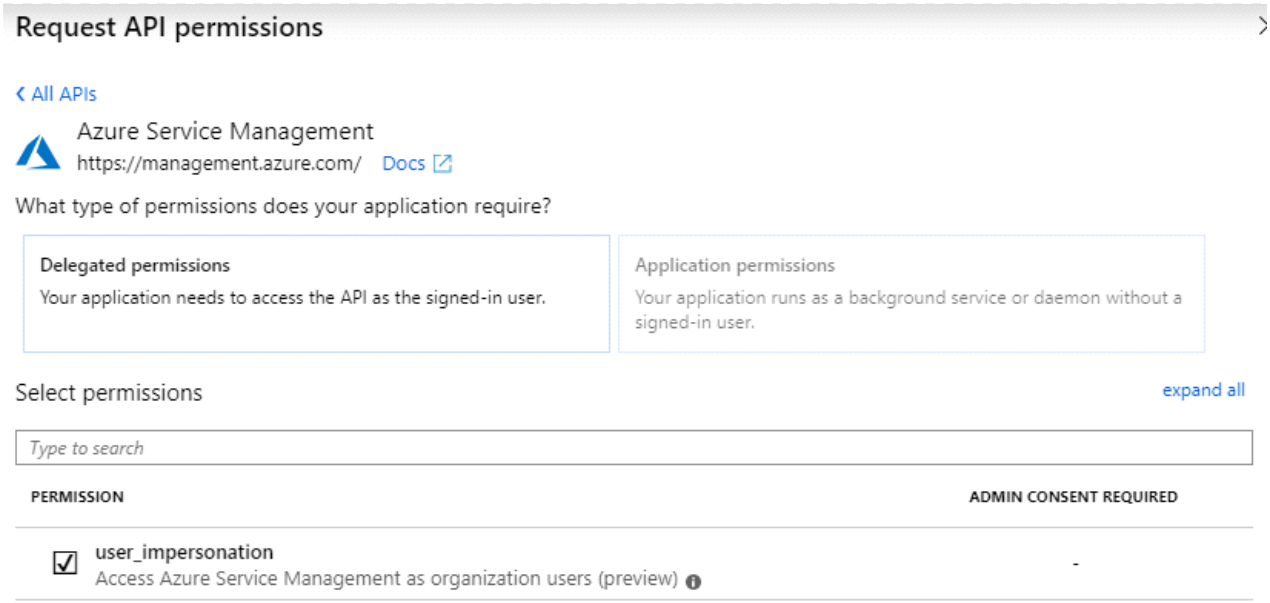
Añada permisos de API de administración de servicios de Windows Azure

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

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

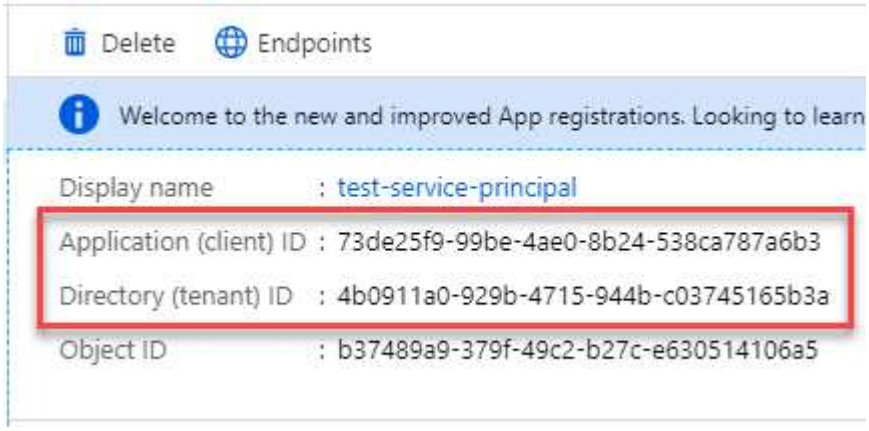


4. Seleccione **Access Azure Service Management como usuarios de organización** y, a continuación, seleccione **Agregar permisos**.



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

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



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

Cree un secreto de cliente

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

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

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. Después de instalar el conector, deberá asociar estas credenciales con el conector de BlueXP.

Paso 5: Instale el conector

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

Antes de empezar

Debe tener lo siguiente:

- Privilegios de root para instalar el conector.
- Detalles sobre un servidor proxy, si se necesita un proxy para el acceso a Internet desde el conector.

  Tiene la opción de configurar un servidor proxy después de la instalación, pero para hacerlo es necesario reiniciar el conector.

  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.

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.

Paso 6: Configure el conector

Inicie sesión o inicie sesión y, a continuación, configure el conector para que funcione con su organización BlueXP .

Pasos

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

   https://ipaddress

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

2. Regístrese o inicie sesión.
3. Después de iniciar sesión, configure BlueXP:
   a. Especifique la organización BlueXP que desea asociar al conector.
   b. Escriba un nombre para el sistema.
   c. En **¿se está ejecutando en un entorno seguro?** mantener el modo restringido desactivado.

      Debe mantener desactivado el modo restringido porque estos pasos describen cómo utilizar BlueXP en modo estándar. (Además, el modo restringido no es compatible cuando el conector está instalado en las instalaciones).

   d. Selecciona **Comenzar**.

Resultado

BlueXP está ahora configurado con el conector que acaba de instalar.

Paso 7: Proporcionar permisos a BlueXP

Después de instalar y configurar Connector, añada sus credenciales del cloud para que BlueXP tenga los permisos necesarios para realizar acciones en AWS o Azure.

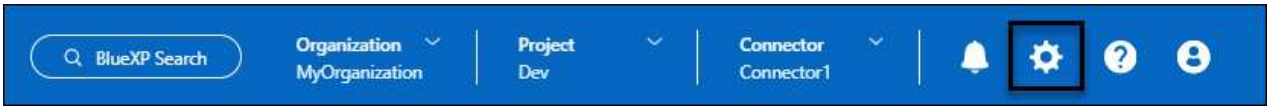
AWS

Antes de empezar

Si acaba de crear estas credenciales en AWS, puede tardar varios minutos en estar disponible para su uso. Espere unos minutos antes de agregar las credenciales a BlueXP.

Pasos

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



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

Resultado

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

Ahora puede ir al "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

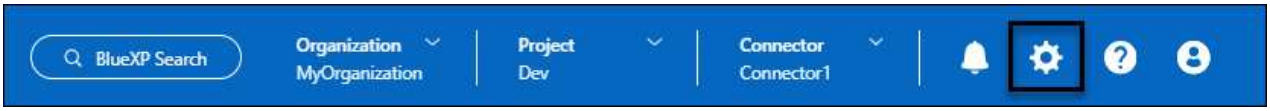
Azure

Antes de empezar

Si acaba de crear estas credenciales en Azure, es posible que tardé unos minutos en poder utilizarlas. Espere unos minutos antes de agregar las credenciales a BlueXP.

Pasos

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



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

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

Resultado

BlueXP ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre. Ahora puede ir al "Consola BlueXP" Para empezar a utilizar el conector con BlueXP.

Información de copyright

Información de la marca comercial