Conectores

BlueXP setup and administration

NetApp
October 25, 2024

Tabla de contenidos

Conectores

Mantener la VM Connector y el sistema operativo

El mantenimiento del sistema operativo en el host del conector es responsabilidad suya. Por ejemplo, debe aplicar actualizaciones de seguridad al sistema operativo en el host del conector siguiendo los procedimientos estándar de su empresa para la distribución del sistema operativo.

Si tiene un conector existente, debe tener en cuenta "Cambios en los sistemas operativos Linux admitidos".

Parches del sistema operativo y el conector

No es necesario detener ningún servicio en el host de Connector al aplicar parches de seguridad del sistema operativo.

Tipo de máquina virtual o instancia

Si creaste un Connector directamente desde BlueXP, BlueXP implementó una instancia de máquina virtual en tu proveedor de nube con una configuración predeterminada. Después de crear el conector, no debe cambiar a una instancia de VM más pequeña que tenga menos CPU o RAM.

Los requisitos de CPU y RAM son los siguientes:

CPU

8 núcleos o 8 vCPU

RAM

32GB

"Obtenga información sobre la configuración predeterminada para el conector".

Parada del inicio de la máquina virtual Connector

Si necesita detener y, a continuación, iniciar Connector VM, debe hacerlo desde la consola de su proveedor de cloud o mediante los procedimientos estándar para la gestión en las instalaciones.

"Tenga en cuenta que el conector debe estar operativo en todo momento".

Conéctese a la máquina virtual de Linux

Si necesita conectarse a la VM de Linux en la que se ejecuta el conector, puede hacerlo utilizando las opciones de conectividad disponibles de su proveedor de cloud.

AWS

Al crear la instancia de Connector en AWS, proporcionó una clave de acceso y una clave secreta de AWS. Es posible usar este par de claves para SSH a la instancia. El nombre de usuario para la instancia de Linux EC2 es ubuntu (para los conectores creados antes de mayo de 2023, el nombre de usuario era EC2-user).

"AWS Docs: Conéctese a su instancia de Linux"

Azure

Cuando creó la máquina virtual de Connector en Azure, especificó un nombre de usuario y optó por autenticarse con una contraseña o clave pública SSH. Utilice el método de autenticación que ha elegido para conectarse a la máquina virtual.

"Azure Docs: SSH en su máquina virtual"

Google Cloud

No puede especificar un método de autenticación al crear un conector en Google Cloud. Sin embargo, puede conectarse a la instancia de VM de Linux mediante Google Cloud Console o Google Cloud CLI (gcloud).

"Google Cloud Docs: Conexión a equipos virtuales Linux"

Cambiar la dirección IP de un conector

Si es necesario para su empresa, puede cambiar la dirección IP interna y la dirección IP pública de la instancia de conector que asigna automáticamente su proveedor de cloud.

Pasos

1. Siga las instrucciones del proveedor de cloud para cambiar la dirección IP local o la dirección IP pública (o ambas) de la instancia de Connector.
2. Si ha cambiado la dirección IP pública y necesita conectarse a la interfaz de usuario local que se ejecuta en el conector, reinicie la instancia del conector para registrar la nueva dirección IP con BlueXP.
3. Si cambió la dirección IP privada, actualice la ubicación de copia de seguridad de los archivos de configuración de Cloud Volumes ONTAP para que las copias de seguridad se envíen a la nueva dirección IP privada del conector.

   Deberá actualizar la ubicación de copia de seguridad de cada sistema Cloud Volumes ONTAP.

   a. En la interfaz de línea de comandos de Cloud Volumes ONTAP, establezca el nivel de privilegio en advanced:

   ```
   set -privilege advanced
   ```

   b. Ejecute el siguiente comando para mostrar el destino de backup actual:

   ```
   system configuration backup settings show
   ```

   c. Ejecute el siguiente comando para actualizar la dirección IP del destino de copia de seguridad:

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

Editar los URI de un conector

Agregue y elimine el identificador uniforme de recursos (URI) de un conector.

Pasos

1. Seleccione la lista desplegable **conector** del encabezado BlueXP.
2. Seleccione **gestionar conectores**.
3. Seleccione el menú de acción de un conector y seleccione **Editar URIs**.
4. Agregue y elimine URIs y, a continuación, seleccione **aplicar**.

Instale un certificado firmado por CA para acceder a la consola basada en web

Cuando se utiliza BlueXP en modo restringido o en modo privado, se puede acceder a la interfaz de usuario desde la máquina virtual de Connector que se implementa en la región de nube o en las instalaciones. De forma predeterminada, BlueXP utiliza un certificado SSL autofirmado para proporcionar acceso HTTPS seguro a la consola basada en web que se ejecuta en el conector. Si así lo requiere su empresa, puede instalar un certificado firmado por una entidad de certificación (CA), la cual ofrece mejor protección de seguridad que un certificado autofirmado. Después de instalar el certificado, BlueXP utiliza el certificado firmado por CA cuando los usuarios acceden a la consola basada en web.

Antes de empezar

Debe crear un conector para poder cambiar la configuración de BlueXP. "Aprenda a crear un conector".

Instale un certificado HTTPS

Instale un certificado firmado por una CA para obtener acceso seguro a la consola basada en web que se ejecuta en el conector.

Acerca de esta tarea

Puede instalar el certificado mediante una de las siguientes opciones:

- Genere una solicitud de firma de certificación (CSR) en BlueXP , envíe la solicitud de certificación a una CA y, a continuación, instale el certificado firmado por CA en el conector.

  El par de claves que BlueXP utiliza para generar la CSR se almacena internamente en el conector. BlueXP recupera automáticamente el mismo par de claves (clave privada) al instalar el certificado en el conector.

- Instale un certificado firmado por CA que ya tenga.

  Con esta opción, la CSR no se genera a través de BlueXP . Se genera la CSR por separado y se almacena la clave privada externamente. Usted proporciona a BlueXP la clave privada al instalar el certificado.

Pasos

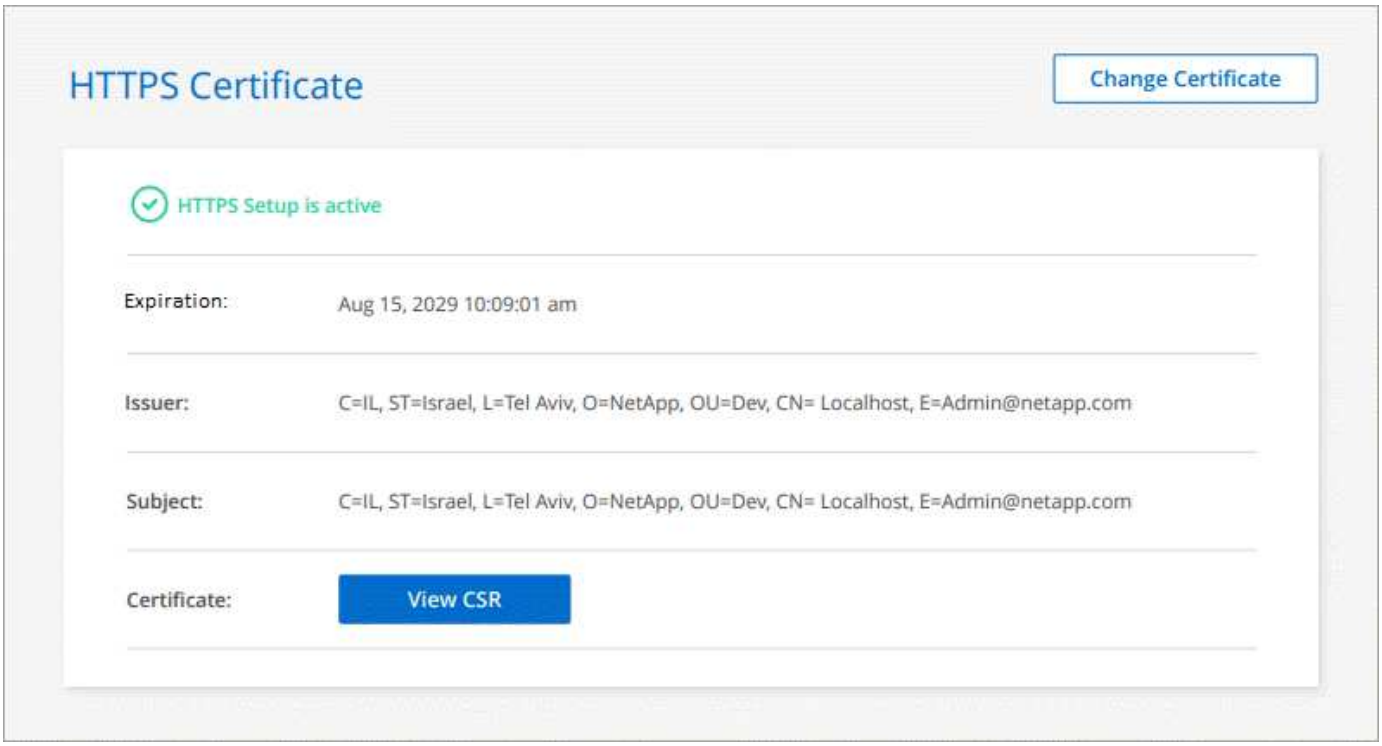
1. En la parte superior derecha de la consola BlueXP, seleccione el icono Configuración y seleccione **Configuración HTTPS**.

2. En la página HTTPS Setup, instale un certificado generando una solicitud de firma de certificación (CSR) o instalando su propio certificado firmado por una CA:

Opción	Descripción
Genere una CSR	a. Introduzca el nombre de host o DNS del host del conector (su nombre común) y, a continuación, seleccione **generar CSR**. BlueXP muestra una solicitud de firma de certificado. b. Utilice la CSR para enviar una solicitud de certificado SSL a una CA. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64. c. Cargue el archivo de certificado y, a continuación, seleccione **instalar**.
Instale su propio certificado firmado por CA	a. Seleccione **instalar certificado firmado por CA**. b. Cargue el archivo de certificado y la clave privada y, a continuación, seleccione **instalar**. El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.

Resultado

Ahora BlueXP utiliza el certificado firmado por CA para proporcionar acceso HTTPS seguro. La siguiente imagen muestra un conector configurado para un acceso seguro:



Renueve el certificado HTTPS de BlueXP

Debe renovar el certificado HTTPS de BlueXP antes de que caduque para garantizar un acceso seguro a la consola BlueXP. Si no renueva el certificado antes de que caduque, aparece una advertencia cuando los usuarios acceden a la consola Web mediante HTTPS.

Pasos

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

   Se muestra información sobre el certificado BlueXP, incluida la fecha de caducidad.

2. Seleccione **Cambiar certificado** y siga los pasos para generar una CSR o instalar su propio certificado firmado por CA.

Resultado

BlueXP utiliza el nuevo certificado firmado por CA para proporcionar acceso HTTPS seguro.

Configure un conector para que utilice un servidor proxy

Si las directivas de la empresa requieren que utilice un servidor proxy para todas las comunicaciones a Internet, deberá configurar los conectores para que utilicen ese servidor proxy. Si no configuró un conector para que utilice un servidor proxy durante la instalación, puede configurar el conector para que utilice ese servidor proxy en cualquier momento.

Configurar el conector para que utilice un servidor proxy proporciona acceso saliente a Internet si no hay disponible una dirección IP pública o una puerta de enlace NAT. Este servidor proxy sólo proporciona el conector con una conexión saliente. No ofrece conectividad para los sistemas Cloud Volumes ONTAP.

Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet de salida para enviar mensajes AutoSupport, BlueXP configura automáticamente esos sistemas Cloud Volumes ONTAP para que utilicen un servidor proxy incluido con 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.

Configuraciones admitidas

- BlueXP admite HTTP y HTTPS.
- El servidor proxy puede estar en la nube o en la red.
- BlueXP no admite servidores proxy transparentes.

Activar un proxy en un conector

Cuando configura un conector para utilizar un servidor proxy, ese conector y los sistemas Cloud Volumes ONTAP que administra (incluidos los mediadores ha), todos utilizan el servidor proxy.

Tenga en cuenta que esta operación reinicia el conector. Asegúrese de que el conector no está realizando ninguna operación antes de continuar.

Pasos

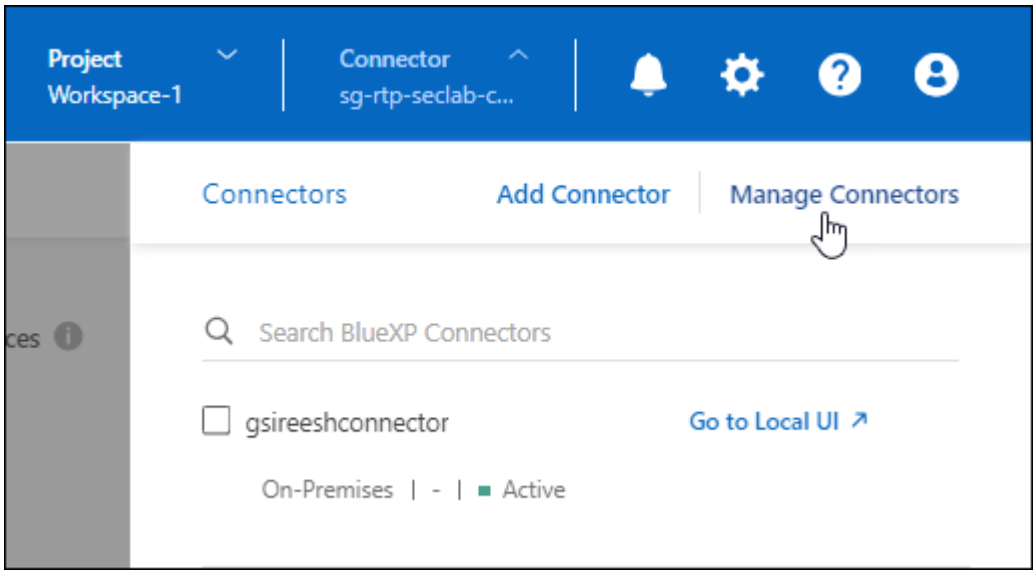
1. Navega a la página **Edit BlueXP Connector**.

   La navegación depende de si utilizas BlueXP en el modo estándar (accedes a la interfaz de BlueXP desde el sitio web de SaaS) o si utilizas BlueXP en el modo restringido o en el modo privado (accedes a la interfaz de BlueXP localmente desde el host de Connector).

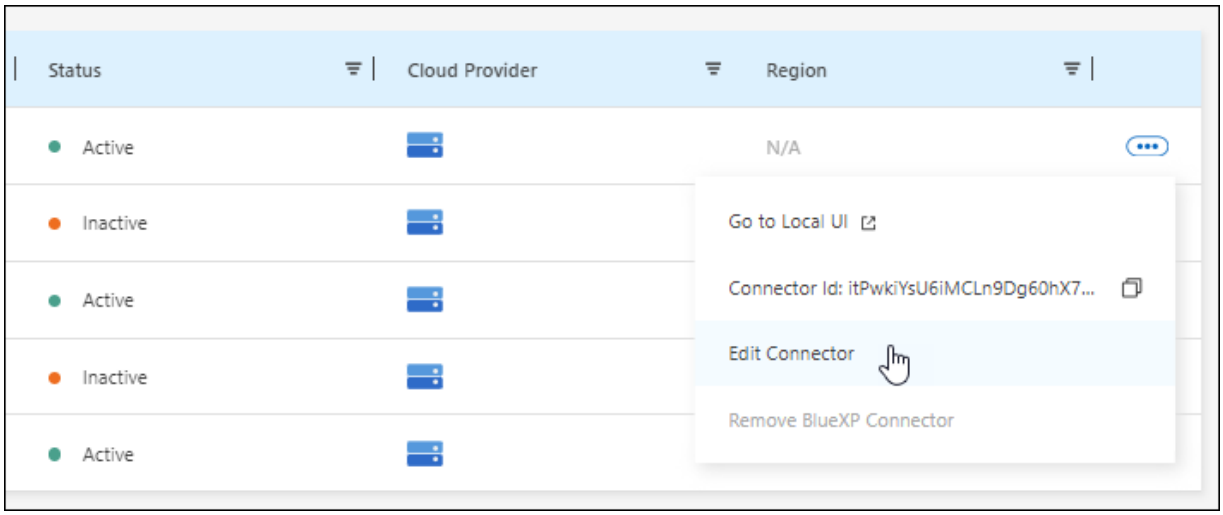
Modo estándar

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **gestionar conectores**.



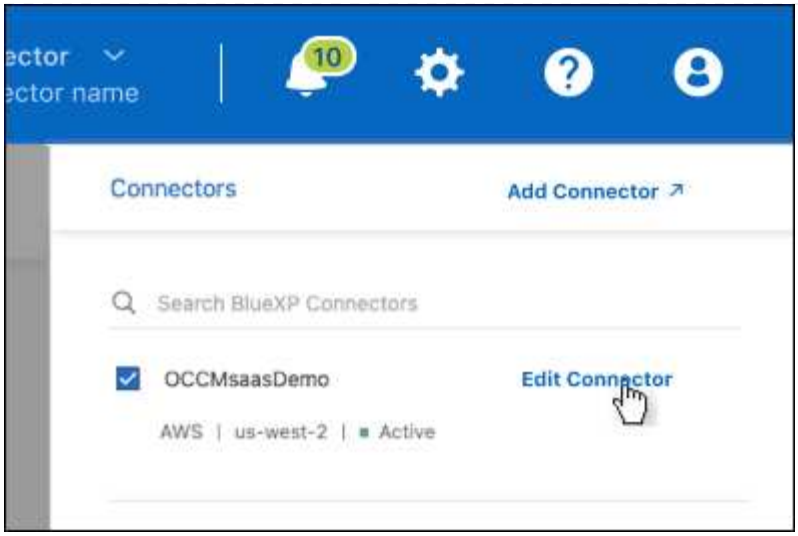
c. Seleccione el menú de acción de un conector y seleccione **Editar conector**.



Modo restringido o privado

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **Editar conector**.



2. Seleccione **Configuración de proxy HTTP**.
3. Configure el proxy:
   a. Seleccione **Activar proxy**.
   b. Especifique el servidor con la sintaxis http://address:port o. https://address:port
   c. Especifique un nombre de usuario y una contraseña si el servidor necesita autenticación básica.

      Tenga en cuenta lo siguiente:

      - El usuario puede ser un usuario local o un usuario de dominio.
      - Para un usuario de dominio, debe introducir el código ASCII para \ de la siguiente manera: Domain-name%92user-name

        Por ejemplo: netapp%92proxy

      - BlueXP no admite contraseñas que incluyan el carácter @.
   d. Seleccione **Guardar**.

Habilite el tráfico de API directo

Si ha configurado un conector para utilizar un servidor proxy, puede habilitar el tráfico API directo en el conector para enviar llamadas API directamente a servicios de proveedores de cloud sin pasar por el proxy. Esta opción es compatible con conectores que se ejecutan en AWS, en Azure o en Google Cloud.

Si deshabilitó el uso de vínculos privados de Azure con Cloud Volumes ONTAP y utiliza extremos de servicio, debe habilitar el tráfico de API directo. De lo contrario, el tráfico no se enrutará correctamente.

"Obtenga más información sobre el uso de un enlace privado de Azure o extremos de servicio con Cloud Volumes ONTAP"

Pasos

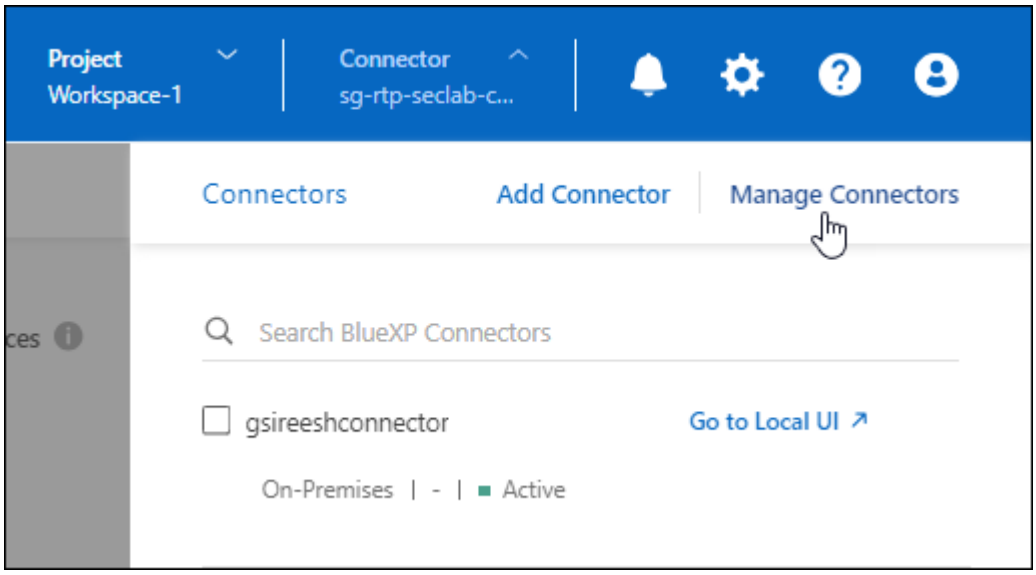
1. Navega a la página **Edit BlueXP Connector**:

La navegación depende de si utilizas BlueXP en el modo estándar (accedes a la interfaz de BlueXP desde el sitio web de SaaS) o si utilizas BlueXP en el modo restringido o en el modo privado (accedes a la interfaz de BlueXP localmente desde el host de Connector).

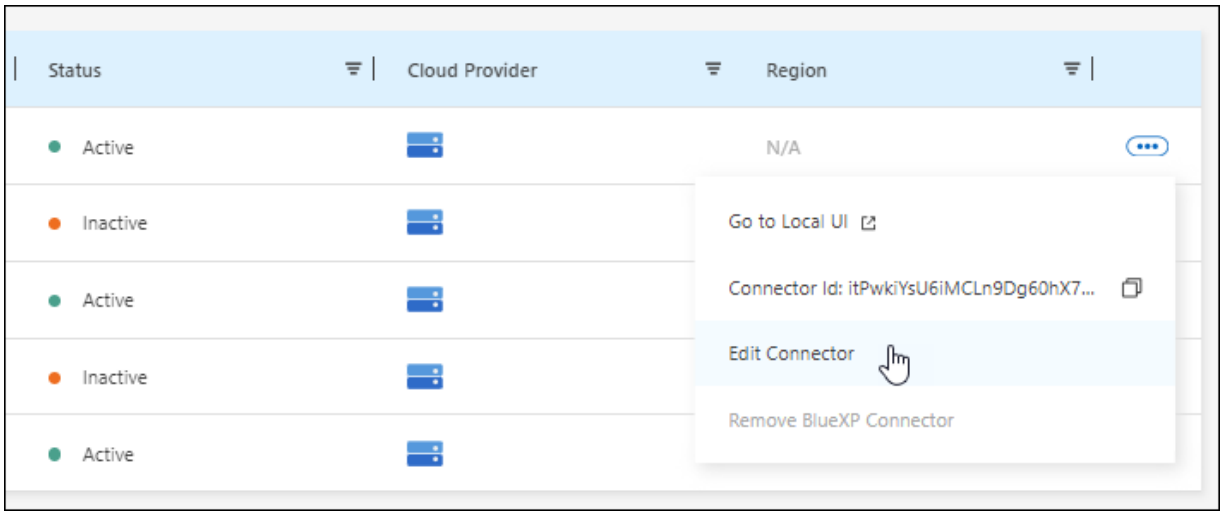
Modo estándar

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **gestionar conectores**.



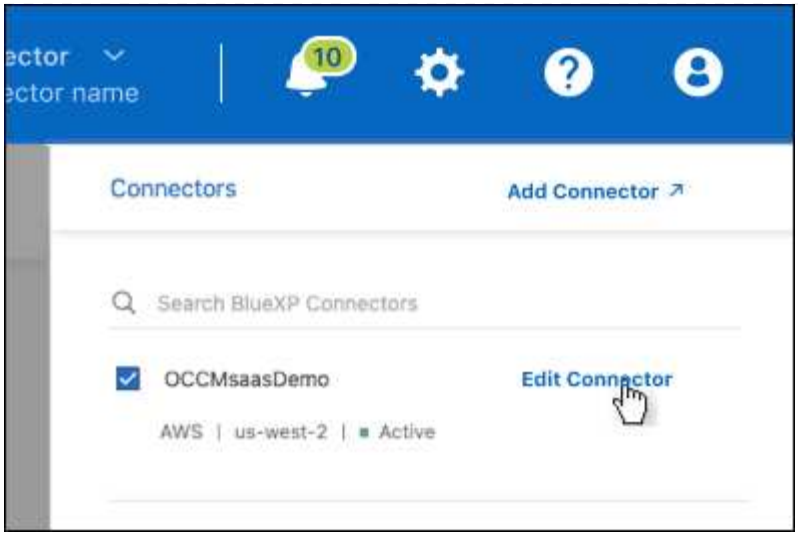
c. Seleccione el menú de acción de un conector y seleccione **Editar conector**.



Modo restringido o privado

a. Seleccione la lista desplegable **conector** del encabezado BlueXP.

b. Seleccione **Editar conector**.



2. Selecciona **Soporte Direct API Traffic**.
3. Seleccione la casilla de verificación para activar la opción y, a continuación, seleccione **Guardar**.

Requiere el uso de IMDSv2 en instancias de Amazon EC2

BlueXP admite el servicio de metadatos de la instancia de Amazon EC2 versión 2 (IMDSv2) con Connector y con Cloud Volumes ONTAP (incluido el mediador para puestas en marcha de alta disponibilidad). En la mayoría de los casos, IMDSv2 se configura automáticamente en instancias de EC2 nuevas. IMDSv1 se activó antes de marzo de 2024. Si las directivas de seguridad lo requieren, es posible que deba configurar manualmente IMDSv2 en las instancias de EC2.

Antes de empezar

- La versión del conector debe ser 3.9.38 o posterior.
- Cloud Volumes ONTAP debe ejecutar una de las siguientes versiones:
  - 9.12.1 P2 (o cualquier parche posterior)
  - 9.13.0 P4 (o cualquier parche posterior)
  - 9.13.1 o cualquier versión posterior a esta versión
- Este cambio requiere que reinicie las instancias de Cloud Volumes ONTAP.
- Estos pasos requieren el uso de la CLI de AWS porque debe cambiar el límite de saltos de respuesta a 3.

Acerca de esta tarea

IMDSv2 proporciona protección mejorada contra vulnerabilidades. "Obtenga más información sobre IMDSv2 en el blog de seguridad de AWS"

El servicio de metadatos de instancia (IMDS) se activa de la siguiente forma en las instancias EC2:

- Para nuevas puestas en marcha de Connector de BlueXP o mediante "Guiones Terraform", IMDSv2 está activado por defecto en la instancia EC2.
- Si inicia una nueva instancia de EC2 en AWS y, a continuación, instala manualmente el software Connector, también se habilita IMDSv2 de forma predeterminada.

- Si inicia Connector desde AWS Marketplace, IMDSv1 está habilitado de forma predeterminada. Puede configurar manualmente IMDSv2 en la instancia de EC2.
- Para los conectores existentes, IMDSv1 sigue siendo compatible, pero puede configurar manualmente IMDSv2 en la instancia EC2 si lo prefiere.
- Para Cloud Volumes ONTAP, IMDSv1 se habilita de forma predeterminada en las instancias nuevas y existentes. Puede configurar manualmente IMDSv2 en las instancias EC2 si lo prefiere.

Pasos

1. Requerir el uso de IMDSv2 en la instancia de conector:

   a. Conéctese a la máquina virtual de Linux para el conector.

      Al crear la instancia de Connector en AWS, proporcionó una clave de acceso y una clave secreta de AWS. Es posible usar este par de claves para SSH a la instancia. El nombre de usuario para la instancia de Linux EC2 es ubuntu (para los conectores creados antes de mayo de 2023, el nombre de usuario era EC2-user).

      "AWS Docs: Conéctese a su instancia de Linux"

   b. Instale la CLI de AWS.

      "AWS Docs: Instale o actualice a la última versión de la CLI de AWS"

   c. Utilice la `aws ec2 modify-instance-metadata-options` Comando para requerir el uso de IMDSv2 y para cambiar el límite de salto de respuesta PUT a 3.

      ejemplo

      ```
      aws ec2 modify-instance-metadata-options \
          --instance-id <instance-id> \
          --http-put-response-hop-limit 3 \
          --http-tokens required \
          --http-endpoint enabled
      ```

      La `http-tokens` El parámetro establece IMDSv2 en Necesario. Cuando `http-tokens` es necesario, también debe establecer `http-endpoint` para activarlo.

2. Requerir el uso de IMDSv2 en instancias de Cloud Volumes ONTAP:

   a. Vaya a la "Consola de Amazon EC2"

   b. En el panel de navegación, selecciona **Instancias**.

   c. Seleccione una instancia de Cloud Volumes ONTAP.

   d. Seleccione **Acciones > Configuración de instancia > Modificar opciones de metadatos de instancia**.

   e. En el cuadro de diálogo **Modificar opciones de metadatos de instancia**, seleccione lo siguiente:

      - Para **servicio de metadatos de instancia**, selecciona **Habilitar**.
      - Para **IMDSv2**, selecciona **Requerido**.

- Seleccione **Guardar**.

f. Repita estos pasos para otras instancias de Cloud Volumes ONTAP, incluido el mediador HA.

g. "Pare e inicie las instancias de Cloud Volumes ONTAP"

Resultado

La instancia de conector y las instancias de Cloud Volumes ONTAP ahora están configuradas para utilizar IMDSv2.

Actualice un conector cuando utilice el modo privado

Si utiliza BlueXP en modo privado, puede actualizar Connector cuando haya una versión más reciente disponible en el sitio de soporte de NetApp.

> Cuando utilizas BlueXP en modo estándar o en modo restringido, no es necesario actualizar manualmente el conector. BlueXP actualiza automáticamente un Connector a la última versión, siempre y cuando el Connector tenga acceso a Internet saliente para obtener la actualización del software.

Acerca de esta tarea

El conector debe reiniciarse durante el proceso de actualización para que la consola basada en Web no esté disponible durante la actualización.

Pasos

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

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

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

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

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

4. Ejecute el script de instalación:

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

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

5. Una vez finalizada la actualización, puede verificar la versión del conector en **Ayuda > Soporte > conector**.

Trabaje con varios conectores

Si utilizas varios conectores, BlueXP te permite alternar entre esos conectores

directamente desde la consola. También puede gestionar un único entorno de trabajo con varios conectores.

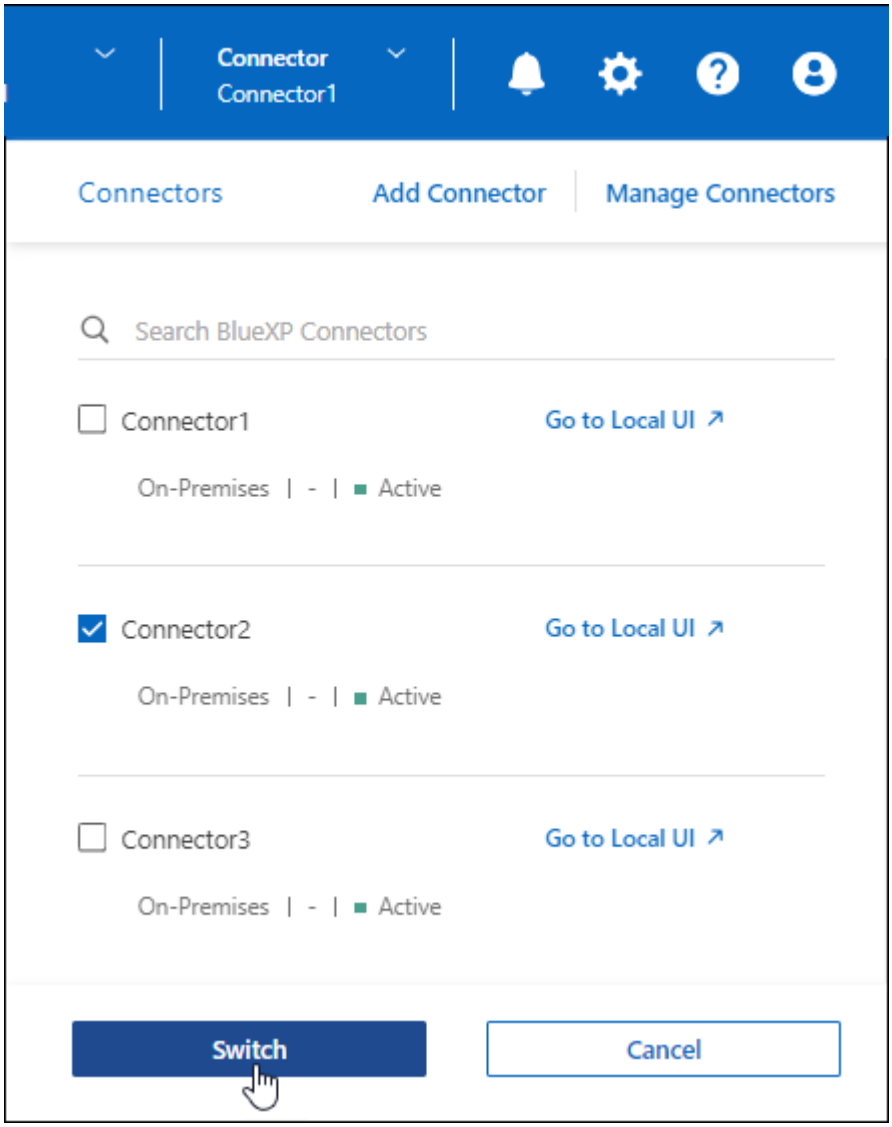
Cambiar entre conectores

Si tiene varios conectores, puede alternar entre ellos para ver los entornos de trabajo asociados a un conector específico.

Por ejemplo, digamos que trabaja en un entorno multicloud. Es posible que tenga un conector en AWS y otro en Google Cloud. Tendría que cambiar entre estos conectores para gestionar los sistemas Cloud Volumes ONTAP que se ejecutan en esas nubes.

Paso

1. Seleccione la lista desplegable **conector**, seleccione otro conector y, a continuación, seleccione **interruptor**.



Resultado

BlueXP actualiza y muestra los entornos de trabajo asociados al conector seleccionado.

Establezca una configuración de recuperación de desastres

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

Pasos

1. Cambie al otro conector que desee gestionar con el entorno de trabajo.
2. Detectar el entorno de trabajo existente.
   - "Agregue sistemas Cloud Volumes ONTAP existentes a BlueXP"
   - "Detectar clústeres de ONTAP"
3. Si gestiona un entorno de trabajo Cloud Volumes ONTAP, seleccione **Configuración > Configuración del conector** y establezca el Modo de gestión de capacidad en **Modo manual**.

   Para evitar problemas de contención, solo el conector principal debe configurarse en **Modo automático**.

   "Obtenga más información sobre el modo de gestión de la capacidad"

Localice y solucione los problemas del conector

Para solucionar los problemas relacionados con el conector, puede trabajar con el soporte de NetApp que puede solicitar el ID del sistema, la versión del conector o los mensajes de AutoSupport más recientes. También puede ver la base de conocimientos de NetApp para solucionar los problemas por sí mismo.

Enlace relacionado

"Obtener ayuda del servicio de soporte de NetApp".

Busque el ID del sistema de un conector

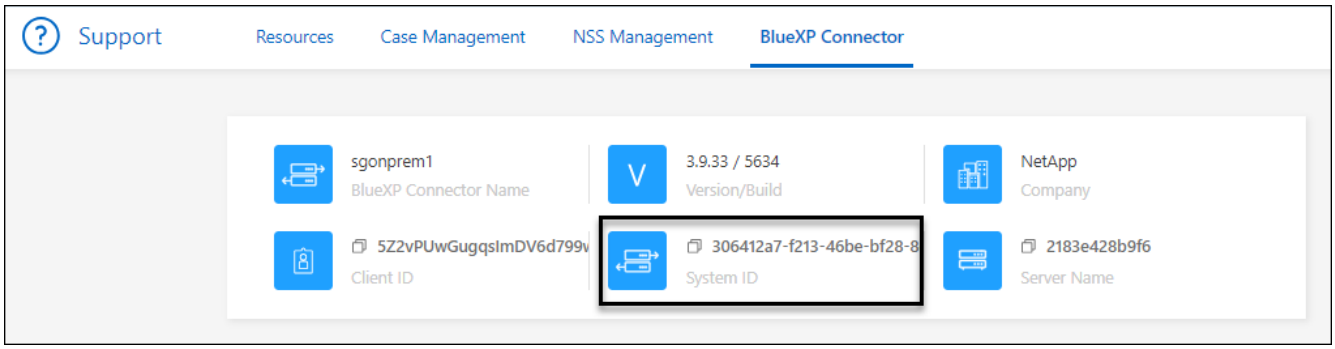
Para ayudarle a comenzar, su representante de NetApp puede pedirle el ID de sistema de su conector. El ID se utiliza normalmente para licencias y solución de problemas.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda.
2. Selecciona **Support > BlueXP Connector**.

   El ID del sistema aparece en la parte superior de la página.

   ejemplo



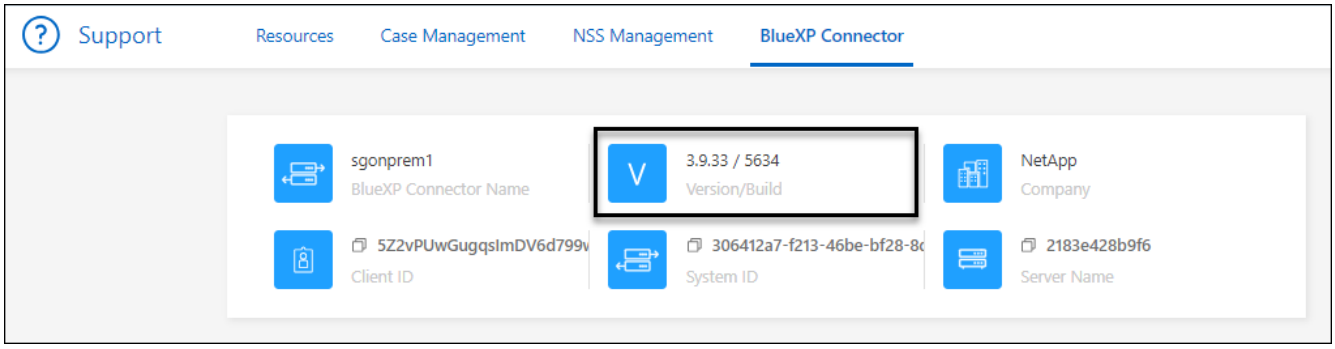
Ver la versión de un conector

Puede ver la versión de su conector para verificar que el conector se actualiza automáticamente a la última versión o porque necesita compartirlo con su representante de NetApp.

Pasos

1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda.
2. Selecciona **Support > BlueXP Connector**.

   La versión se muestra en la parte superior de la página.

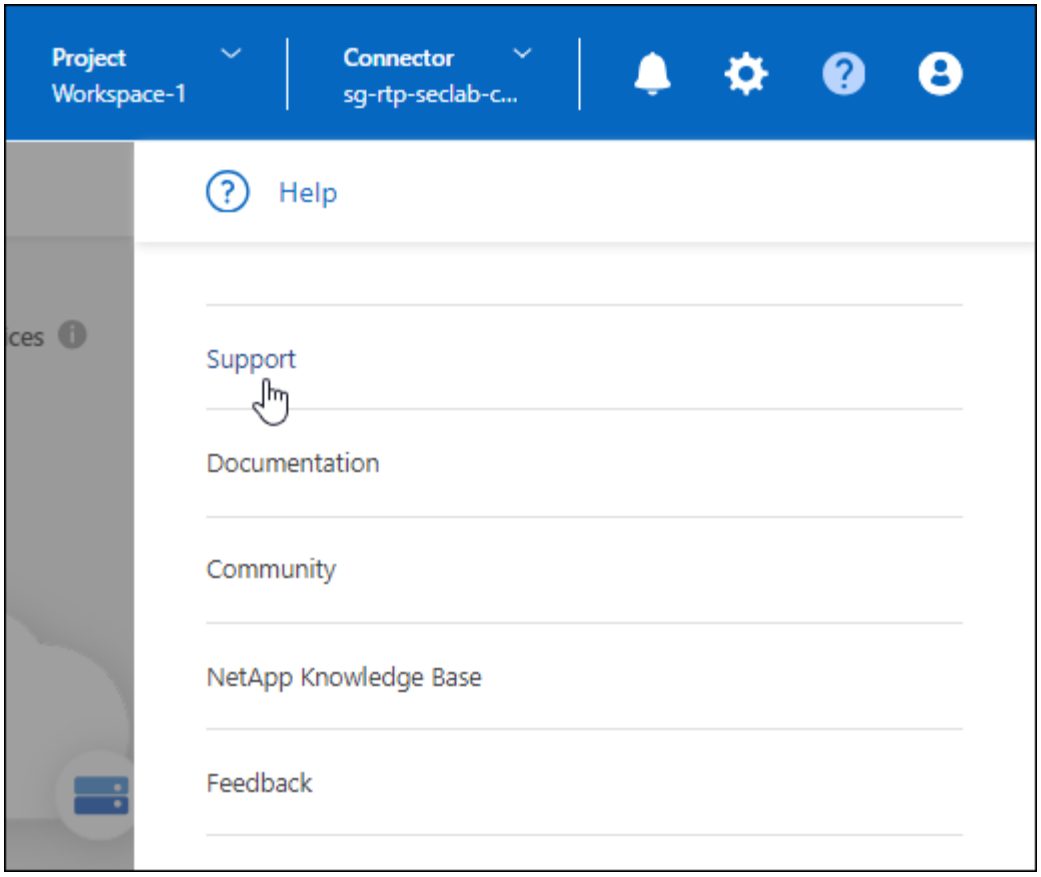


Descargar o enviar un mensaje de AutoSupport

Si tiene problemas, es posible que el personal de NetApp le solicite enviar un mensaje de AutoSupport al soporte de NetApp para la solución de problemas.

Pasos

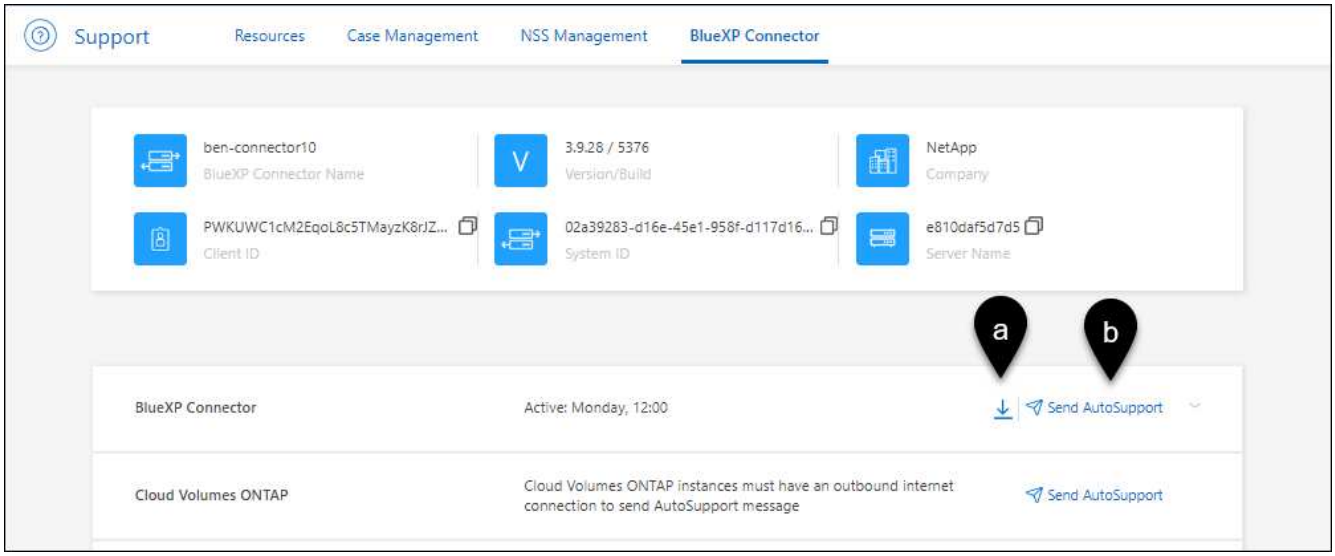
1. En la parte superior derecha de la consola de BlueXP, seleccione el icono Ayuda y seleccione **Soporte**.



2. Seleccione **conector BlueXP**.
3. En función de cómo necesite enviar la información al soporte de NetApp, seleccione una de las siguientes opciones:

   a. Seleccione la opción para descargar el mensaje de AutoSupport en el equipo local. Luego, puede enviarlo al soporte de NetApp mediante un método preferido.

   b. Seleccione **Enviar AutoSupport** para enviar directamente el mensaje al soporte de NetApp.



Solucione los fallos de descarga al utilizar una puerta de enlace NAT de Google Cloud

El conector descarga automáticamente las actualizaciones de software de Cloud Volumes ONTAP. La descarga puede fallar si la configuración utiliza una puerta de enlace de NAT de Google Cloud. Puede corregir este problema limitando el número de partes en las que se divide la imagen de software. Este paso se debe completar mediante la API de BlueXP.

Paso

1. Envíe una solicitud PUT a /occm/config con el siguiente JSON como cuerpo:

   ```
   {
     "maxDownloadSessions": 32
   }
   ```

   El valor para *maxDownloadSessions* puede ser 1 o cualquier entero mayor que 1. Si el valor es 1, la imagen descargada no se dividirá.

   Tenga en cuenta que 32 es un valor de ejemplo. El valor que debe utilizar depende de la configuración de NAT y del número de sesiones que puede tener simultáneamente.

"Obtenga más información acerca de la llamada a la API /occm/config"

Obtenga ayuda de la base de conocimientos de NetApp

"Ver la información para la solución de problemas creada por el equipo de soporte de NetApp".

Desinstale y retire el conector

Desinstale el software del conector para solucionar problemas o para quitar el software del host de forma permanente. Los pasos que debe seguir dependen del modo de despliegue que esté utilizando. Cuando se ha eliminado un Connector de tu entorno, puedes eliminarlo de BlueXP.

"Obtenga más información sobre los modos de implementación de BlueXP".

Desinstale Connector cuando utilice el modo estándar o restringido

Si utiliza BlueXP en modo estándar o en modo restringido (es decir, el host de Connector tiene conectividad saliente), siga los pasos que se describen a continuación para desinstalar el software Connector.

Pasos

1. Conéctese a la máquina virtual de Linux para el conector.
2. Desde el host Linux, ejecute el script de desinstalación:

   ```
   /opt/application/netapp/service-manager-2/uninstall.sh [silent]
   ```

   silent ejecuta la secuencia de comandos sin que se le solicite confirmación.

Resultado

El software Connector ahora se desinstala del host Linux.

Desinstale Connector cuando utilice el modo privado

Si utilizas BlueXP en modo privado (es decir, el host del conector tiene conectividad saliente *no*), debes seguir los pasos que se indican a continuación para desinstalar el software Connector.

Paso

1. Conéctese a la máquina virtual de Linux para el conector.
2. Desde el host Linux, ejecute los siguientes comandos:

```
/opt/application/netapp/ds/cleanup.sh
rm -rf /opt/application/netapp/ds
```

Resultado

El software Connector ahora se desinstala del host Linux.

Quitar conectores de BlueXP

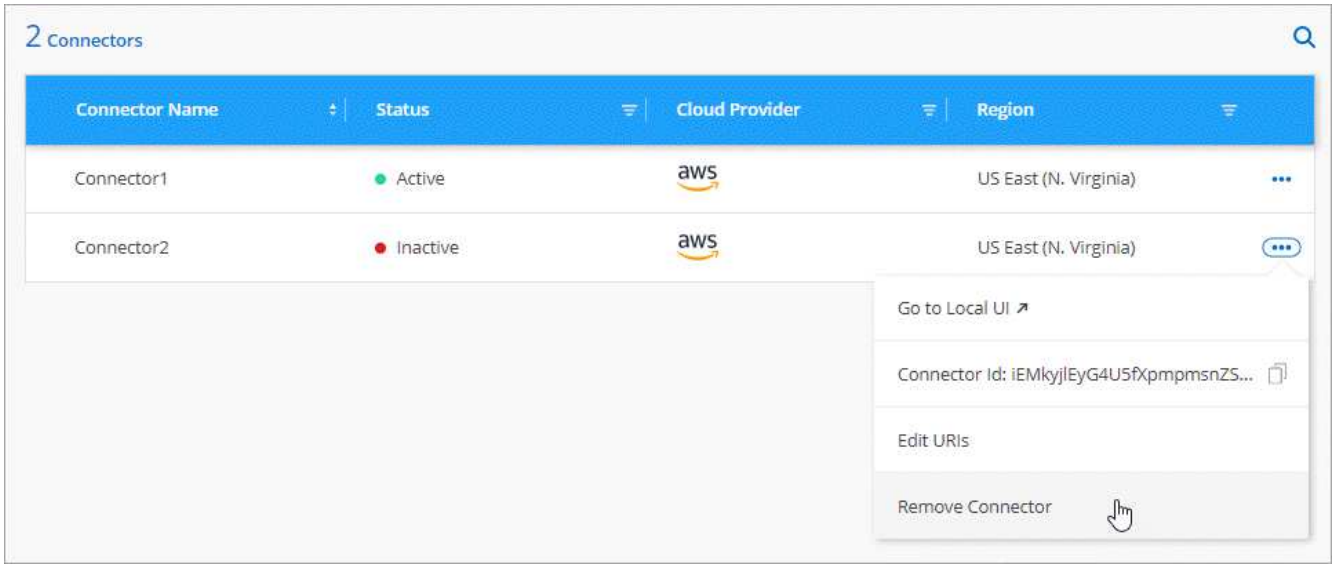
Si un conector está inactivo, puede eliminarlo de la lista de conectores de BlueXP. Puede hacerlo si ha eliminado la máquina virtual conector o si ha desinstalado el software conector.

Tenga en cuenta lo siguiente sobre la extracción de un conector:

- Esta acción no elimina la máquina virtual.
- Esta acción no se puede revertir—una vez que se quita un conector de BlueXP, no se puede volver a agregar.

Pasos

1. Seleccione la lista desplegable **conector** del encabezado BlueXP.
2. Seleccione **gestionar conectores**.
3. Seleccione el menú de acción de un conector inactivo y seleccione **Quitar conector**.



4. Introduzca el nombre del conector que desea confirmar y, a continuación, seleccione **Quitar**.

Resultado

BlueXP quita el conector de sus registros.

Configuración predeterminada del conector

Es posible que desee obtener más información sobre la configuración del conector antes de implementarlo o si necesita solucionar cualquier problema.

Configuración predeterminada con acceso a Internet

Los siguientes detalles de configuración se aplican si ha implementado el conector desde BlueXP, desde el mercado del proveedor de la nube o si ha instalado manualmente el conector en un host Linux local que tenga acceso a Internet.

Detalles de AWS

Si implementó el conector desde BlueXP o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de instancia de EC2 es t3.2xlarge.
- El sistema operativo de la imagen es Ubuntu 22,04 LTS.

  El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El nombre de usuario para la instancia de Linux EC2 es ubuntu (para los conectores creados antes de mayo de 2023, el nombre de usuario era EC2-user).
- El disco del sistema predeterminado es un disco gp2 de 100 GIB.

Detalles de Azure

Si implementó el conector desde BlueXP o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de máquina virtual es Standard_D8s_v3.
- El sistema operativo de la imagen es Ubuntu 22,04 LTS.

  El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El disco del sistema predeterminado es un disco SSD premium de 100 GIB.

Detalles de Google Cloud

Si implementó el Connector de BlueXP, tenga en cuenta lo siguiente:

- La instancia del equipo virtual es n2-standard-8.
- El sistema operativo de la imagen es Ubuntu 22,04 LTS.

El sistema operativo no incluye una GUI. Debe utilizar un terminal para acceder al sistema.

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El disco del sistema predeterminado es un disco SSD persistente de 100 GIB.

Carpeta de instalación

La carpeta de instalación del conector se encuentra en la siguiente ubicación:

/opt/aplicación/netapp/cloudmanager

Archivos de registro

Los archivos de registro se encuentran en las siguientes carpetas:

- /opt/application/netapp/cloudmanager/log
  o.
- /opt/application/netapp/service-manager-2/logs (a partir de las nuevas instalaciones de 3.9.23)

  Los registros de estas carpetas proporcionan detalles sobre el conector.

- /opt/aplicación/netapp/cloudmanager/docker_occm/data/log

  Los registros de esta carpeta proporcionan detalles sobre los servicios en la nube y el servicio BlueXP que se ejecuta en el conector.

Servicio de conectores

- El servicio BlueXP se llama occm.
- El servicio occm depende del servicio MySQL.

  Si el servicio MySQL está inactivo, entonces el servicio occm también está inactivo.

Puertos

El conector utiliza los siguientes puertos en el host Linux:

- 80 para acceso HTTP
- 443 para el acceso HTTPS

Configuración predeterminada sin acceso a Internet

La siguiente configuración se aplica si instaló manualmente el conector en un host Linux local que no tiene acceso a Internet. "Obtenga más información sobre esta opción de instalación".

- La carpeta de instalación del conector se encuentra en la siguiente ubicación:

  /opt/aplicación/netapp/ds

- Los archivos de registro se encuentran en las siguientes carpetas:

  /var/lib/docker/volumes/ds_occmdata/_data/log

Los registros de esta carpeta proporcionan detalles sobre las imágenes de conector y Docker.

- Todos los servicios se ejecutan en contenedores Docker

  Los servicios dependen del servicio docker Runtime que se esté ejecutando

- El conector utiliza los siguientes puertos en el host Linux:
  - 80 para acceso HTTP
  - 443 para el acceso HTTPS