



## **Conectores**

### **Set up and administration**

NetApp  
March 10, 2023

# Tabla de Contenido

- Conectores ..... 1
  - Puesta en marcha avanzada ..... 1
  - Búsqueda del ID del sistema de un conector ..... 16
  - Gestión de conectores existentes ..... 17
  - Gestión de un certificado HTTPS para un acceso seguro ..... 24
  - Configure un conector para que utilice un servidor proxy ..... 26
  - Configuración predeterminada del conector ..... 28

# Conectores

## Puesta en marcha avanzada

### Cree un conector desde AWS Marketplace

Para una región comercial de AWS, lo mejor es crear un conector directamente desde BlueXP, pero puede ejecutar un conector desde AWS Marketplace, si lo prefiere. Para regiones gubernamentales de AWS, no es posible poner en marcha el conector en una región gubernamental desde el sitio web BlueXP SaaS, por lo que la mejor opción es hacerlo desde AWS Marketplace.



También puede descargar e instalar el software Connector en un host Linux existente en su red o en la nube. ["Aprenda a instalar el conector en un host Linux existente"](#).

### Cree el conector en una región comercial de AWS

Puede iniciar la instancia de Connector en una región comercial de AWS directamente desde la oferta de AWS Marketplace para BlueXP.

#### Antes de empezar

El usuario de IAM que crea el conector debe tener permisos de AWS Marketplace para suscribirse y cancelar su suscripción.

#### Pasos

1. Configure permisos en AWS:
  - a. Desde la consola IAM, cree las directivas necesarias copiando y pegando el contenido de ["Políticas de IAM para el conector"](#).
  - b. Cree un rol IAM con el tipo de rol Amazon EC2 y adjunte las políticas que creó en el paso anterior al rol.
2. Vaya a la ["Página de BlueXP en AWS Marketplace"](#) Para desplegar el conector desde un AMI:
3. En la página Marketplace, haga clic en **continuar a Suscribirse** y luego haga clic en **continuar a Configuración**.



4. Cambie cualquiera de las opciones predeterminadas y haga clic en **continuar a Iniciar**.
5. En **elegir acción**, seleccione **Iniciar a través de EC2** y, a continuación, haga clic en **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**.

6. Siga las instrucciones para configurar y desplegar la instancia:
  - **Nombre y etiquetas:** Introduzca un nombre y etiquetas para la instancia.
  - **Aplicación y OS Image:** Omitir esta sección. El conector AMI ya está seleccionado.
  - **Tipo de instancia:** En función de la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.xlarge).

"Revise los requisitos de la instancia".

- **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 firewall que habilite los métodos de conexión necesarios para la instancia del conector: SSH, HTTP y HTTPS.
- **Configurar almacenamiento:** Mantenga las opciones de almacenamiento predeterminadas.
- **Detalles avanzados:** En **perfil de instancia de IAM**, elija la función de IAM que creó en el paso 1.
- **Resumen:** Revise el resumen y haga clic en **Iniciar instancia**.

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

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

`https://ipaddress[]`

8. Después de iniciar sesión, configure el conector:

- a. Especifique la cuenta de NetApp que desea asociar al conector.

["Obtenga más información acerca de las cuentas de NetApp"](#).

- b. Escriba un nombre para el sistema.

9. Abra un explorador web y vaya a <https://console.bluexp.netapp.com> Para empezar a utilizar el conector con BlueXP.

## Resultado

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

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

## Cree el conector en una región gubernamental de AWS

Para poner en marcha Connector en una región AWS Government, debe ir al servicio EC2 y seleccionar la oferta BlueXP en AWS Marketplace.

## Pasos

1. Configure permisos en AWS:
  - a. Desde la consola IAM, cree su propia directiva copiando y pegando el contenido de ["Política de IAM para el conector"](#).
  - b. Cree un rol IAM con el tipo de rol Amazon EC2 y asocie la política que ha creado en el paso anterior al rol.
2. Vaya a la oferta de BlueXP en AWS Marketplace.

El usuario de IAM debe disponer de permisos de AWS Marketplace para suscribirse y cancelar la suscripción.

- a. Abra el servicio EC2 y seleccione **Iniciar instancia**.
- b. Seleccione **AWS Marketplace**.

c. Busque BlueXP y seleccione la oferta.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace, or you can select one of your own AMIs.

Search by Systems Manager parameter

Quick Start My AMIs AWS Marketplace Community AMIs Categories

Q bluexp

**NetApp** **BlueXP - Manual Installation without access keys**

★★★★★ (6) | 3.9.23 | By NetApp, Inc.

Linux/Unix, Red Hat Enterprise Linux Red Hat Linux | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 11/17/22

Read below for instructions on how to deploy Cloud Volumes ONTAP.

[More info](#)

**Select**

d. Haga clic en **continuar**.

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

- **Elija un tipo de instancia:** En función de la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.xlarge).

"Revise los requisitos de la instancia".

- **Configurar detalles de instancia:** Seleccione un VPC y una subred, elija la función de IAM que creó en el paso 1, habilite la protección de terminación (recomendado) y elija cualquier otra opción de configuración que cumpla sus requisitos.

**Number of instances** ⓘ 1 [Launch into Auto Scaling Group](#) ⓘ

**Purchasing option** ⓘ ☐ Request Spot instances

**Network** ⓘ vpc-a76d91c2 | VPC4QA (default) ⓘ [Create new VPC](#)

**Subnet** ⓘ subnet-39536c13 | QASubnet1 | us-east-1b ⓘ [Create new subnet](#)

155 IP Addresses available

**Auto-assign Public IP** ⓘ Enable ⓘ

**Placement group** ⓘ ☐ Add instance to placement group

**Capacity Reservation** ⓘ Open ⓘ [Create new Capacity Reservation](#)

**IAM role** ⓘ Cloud\_Manager ⓘ [Create new IAM role](#)

**CPU options** ⓘ ☐ Specify CPU options

**Shutdown behavior** ⓘ Stop ⓘ

**Enable termination protection** ⓘ ☒ Protect against accidental termination

**Monitoring** ⓘ ☐ Enable CloudWatch detailed monitoring

[Additional charges apply.](#)

- **almacenamiento:** Mantenga las opciones de almacenamiento predeterminadas.

- **Agregar etiquetas:** Introduzca etiquetas para la instancia, si lo desea.
- **Configurar grupo de seguridad:** Especifique los métodos de conexión necesarios para la instancia de conector: SSH, HTTP y HTTPS.
- **Revisión:** Revise sus selecciones y haga clic en **Iniciar**.

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

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

`https://ipaddress[]`

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

## Resultado

El conector ahora está instalado y configurado con su cuenta de NetApp.

Siempre que desee utilizar BlueXP, abra el explorador Web y conéctese a la dirección IP de la instancia de Connector: `https://ipaddress[]`

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

## Abra el puerto 3128 para los mensajes de AutoSupport

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

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

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

## Cree un conector desde Azure Marketplace

Para una región comercial de Azure, lo mejor es crear un conector directamente desde BlueXP, pero puede ejecutar un conector desde Azure Marketplace, si lo prefiere. Para regiones gubernamentales de Azure, no es posible poner en marcha Connector en una región gubernamental desde el sitio web BlueXP SaaS, por lo que la mejor opción es hacerlo desde Azure Marketplace.



También puede descargar e instalar el software Connector en un host Linux existente en su red o en la nube. ["Aprenda a instalar el conector en un host Linux existente"](#).

## Creación de un conector en Azure

Implemente el conector en Azure con la imagen en Azure Marketplace y después inicie sesión en el conector para especificar su cuenta de NetApp.

### Pasos

1. Vaya a la página NetApp Connector VM del Azure Marketplace.
  - ["Página de Azure Marketplace para regiones comerciales"](#)
  - ["Página de Azure Marketplace para regiones gubernamentales de Azure"](#)
2. Haga clic en **Get Now** y, a continuación, haga clic en **Continue**.
3. En el portal de Azure, haga clic en **Crear** y siga los pasos para configurar la máquina virtual.

Tenga en cuenta lo siguiente al configurar la máquina virtual:

- El conector puede tener un rendimiento óptimo tanto con discos HDD como SSD.
- Elija un tamaño de máquina virtual que cumpla los requisitos de CPU y RAM. Recomendamos DS3 v2.

["Revise los requisitos de las máquinas virtuales"](#).

- Para el grupo de seguridad de red, el conector requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

["Obtenga más información sobre las reglas de grupo de seguridad para el conector"](#).

- En **Gestión**, active **identidad administrada asignada por el sistema** para el conector seleccionando **On**.

Esta configuración es importante porque una identidad administrada permite que la máquina virtual Connector se identifique a sí misma en Azure Active Directory sin proporcionar credenciales. ["Obtenga más información sobre las identidades gestionadas para recursos de Azure"](#).

4. En la página **revisar + crear**, revise las selecciones y haga clic en **Crear** 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 cuenta de NetApp que desea asociar al conector.

["Obtenga más información acerca de las cuentas de NetApp"](#).

- b. Escriba un nombre para el sistema.

### Resultado



El conector ahora está instalado y configurado con su cuenta de NetApp.

Si el conector está en una región comercial de Azure, abra un explorador web y vaya a <https://console.bluexp.netapp.com> Para empezar a utilizar el conector con BlueXP.

Si Connector se encuentra en una región gubernamental de Azure, puede utilizar BlueXP abriendo su navegador web y conectándose a la dirección IP de la instancia de Connector: [https://ipaddress\[\]](https://ipaddress[])

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

## Concesión de permisos de Azure

Cuando implementó Connector en Azure, debería haber habilitado un "identidad administrada asignada por el sistema". Ahora debe conceder los permisos de Azure necesarios creando una función personalizada y, a continuación, asignando la función a la máquina virtual Connector para una o más suscripciones.

### Pasos

1. Crear un rol personalizado:
  - 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 el rol a la máquina virtual conector para una o más suscripciones:

- a. Abra el servicio **Suscripciones** y seleccione la suscripción en la que desea implementar sistemas Cloud Volumes ONTAP.
- b. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de funciones**.
- c. En la ficha **rol**, seleccione el rol **operador BlueXP** y haga clic en **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.

- d. En la ficha **Miembros**, realice los siguientes pasos:
  - Asignar acceso a una **identidad administrada**.
  - Haga clic en **Seleccionar miembros**, seleccione la suscripción en la que se creó la máquina virtual Connector, elija **máquina virtual** y, a continuación, seleccione la máquina virtual Connector.
  - Haga clic en **Seleccionar**.
  - Haga clic en **Siguiente**.
- e. Haga clic en **revisar + asignar**.
- f. Si desea implementar Cloud Volumes ONTAP desde suscripciones adicionales, cambie a esa suscripción y repita estos pasos.

## Resultado

Connector ahora tiene los permisos que necesita para gestionar recursos y procesos en su entorno de cloud público. BlueXP utilizará este conector automáticamente cuando cree nuevos entornos de trabajo. Pero si tiene más de un conector, necesitará ["alterne entre ellos"](#).

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

### **Abra el puerto 3128 para los mensajes de AutoSupport**

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

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

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

### **Instale el conector en un host Linux existente que tenga acceso a Internet**

La forma más común de crear un conector es directamente desde BlueXP o desde el mercado de un proveedor de la nube. Pero tiene la opción de descargar e instalar el software Connector en un host Linux existente en su red o en la nube. Estos pasos son específicos de los hosts que tienen acceso a Internet.

["Obtenga información sobre otras formas de desplegar un conector"](#).



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

### **Verifique 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.

#### **Se requiere un host dedicado**

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

#### **CPU**

4 núcleos o 4 vCPU

#### **RAM**

14 GB

#### **Tipo de instancia de AWS EC2**

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

#### **Tamaño de la máquina virtual de Azure**

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

## Tipo de máquina GCP

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

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

## Sistemas operativos compatibles

- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6 y 8.7

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

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

## Hipervisor

Un hipervisor de configuración básica o alojado certificado Ejecute CentOS o Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"^]

## Espacio en disco en /opt

Debe haber 100 GiB de espacio disponibles

## Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

## Motor Docker

Se requiere Docker Engine versión 19.3.1 o posterior en el host antes de instalar el conector. "[Ver las instrucciones de instalación](#)"

## Acceso a Internet de salida

El instalador del conector debe acceder a las siguientes direcciones URL durante el proceso de instalación:

- <https://support.netapp.com>
- <https://mysupport.netapp.com>
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://cloudmanagerinfraprod.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net)

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.

## Instale el conector

Después de verificar que tiene un host Linux compatible, puede obtener el software Connector y luego instalarlo.

## Lo que necesitará

- 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. Son compatibles con HTTP y HTTPS.

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

- Un certificado firmado por CA, si el servidor proxy utiliza HTTPS.

## Acerca de esta tarea

- La instalación instala las herramientas de línea de comandos de AWS (awscli) para habilitar los procedimientos de recuperación del soporte de NetApp.

Si recibe un mensaje que ha fallado al instalar el awscli, puede ignorar el mensaje de forma segura. El conector puede funcionar correctamente sin las herramientas.

- 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. Compruebe que docker está activado y en ejecución.

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

2. 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.

3. Descargue el software del conector de "[Sitio de soporte de NetApp](#)"Y, a continuación, cópielo en el host Linux.

Debe descargar el instalador de Connector que se ha diseñado para su uso en la red o en la nube.

4. Asigne permisos para ejecutar el script.

```
chmod +x OnCommandCloudManager-V3.9.23
```

5. Ejecute el script de instalación.

```
./OnCommandCloudManager-V3.9.23 --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:

```
./OnCommandCloudManager-V3.9.23 --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://username:password@address:port
- https://address:port
- https://username:password@address:port

--cacert especifica un certificado firmado por CA que se utilizará para el acceso HTTPS entre el conector y el servidor proxy. Este parámetro solo es obligatorio si se especifica un servidor proxy HTTPS.

## 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.

## Configure el conector

Regístrese o inicie sesión y, a continuación, configure el conector para que funcione con su cuenta.

## 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. Si ha instalado Connector en Google Cloud, configure una cuenta de servicio que tenga los permisos que BlueXP necesita para crear y gestionar sistemas Cloud Volumes ONTAP en proyectos.
  - a. ["Crear un rol en GCP"](#) esto incluye los permisos definidos en la ["Política de conectores para GCP"](#).
  - b. ["Cree una cuenta de servicio de GCP y aplique el rol personalizado que acaba de crear"](#).
  - c. ["Asocie esta cuenta de servicio a la máquina virtual del conector"](#).
  - d. Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, ["Conceda acceso agregando la cuenta de servicio con la función BlueXP a ese proyecto"](#). Deberá repetir este paso con cada proyecto.
4. Después de iniciar sesión, configure BlueXP:
  - a. Especifique la cuenta de NetApp que desea asociar al conector.

["Obtenga más información acerca de las cuentas de NetApp"](#).

- b. Escriba un nombre para el sistema.

## Resultado

El conector ahora está instalado y configurado con su cuenta de NetApp. BlueXP utilizará este conector automáticamente cuando cree nuevos entornos de trabajo.

## Después de terminar

Configure permisos para que BlueXP pueda gestionar recursos y procesos en su entorno de cloud público:

- AWS: ["Configure una cuenta de AWS y, a continuación, agréguela a BlueXP"](#)
- Azure: ["Configure una cuenta de Azure y añádala a BlueXP"](#)
- Google Cloud: Consulte el paso 3 anterior

## Instale el conector en una ubicación sin acceso a Internet

Puede instalar el conector en una ubicación que tenga un aislamiento completo de Internet, ya sea en las instalaciones o en una región de la nube. A continuación, puede utilizar los servicios BlueXP que son compatibles con ese entorno.

### Información general en las instalaciones

En un entorno local sin Internet, puede utilizar BlueXP para detectar clústeres de ONTAP en las instalaciones, replicar datos entre ellos, realizar backups de volúmenes con Cloud Backup y analizarlos con Cloud Data Sense. Ningún otro servicio BlueXP es compatible con este tipo de despliegue, excepto con la cartera digital.

### Información general sobre el cloud

En una región de cloud sin Internet, puede usar BlueXP para poner en marcha sistemas Cloud Volumes ONTAP y detectar clústeres de ONTAP en las instalaciones (si hay una conexión de su entorno cloud a su entorno local). Ningún otro servicio BlueXP es compatible con este tipo de despliegue, excepto con la cartera digital.

La región del cloud puede ser una región en la que haya agencias estadounidenses seguras como AWS C2S/SC2S, Azure IL6 o cualquier región comercial.

Estas instrucciones de instalación son específicas para el caso de uso descrito anteriormente. ["Obtenga información sobre otras formas de desplegar un conector"](#).

### Verifique 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.

### Se requiere un host dedicado

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

### CPU

4 núcleos o 4 vCPU

## RAM

14 GB

## Sistemas operativos compatibles

- CentOS 7.6, 7.7, 7.8 y 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6 y 8.7

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

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

## Hipervisor

Un hipervisor de configuración básica o alojado certificado Ejecute CentOS o Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Red Hat Solution: ¿Qué hipervisores están certificados para ejecutar Red Hat Enterprise Linux?"^]

## Tipo de disco

Se requiere un SSD

## Espacio en disco en /opt

Debe haber 100 GiB de espacio disponibles

## Espacio en disco en /var

Debe haber 20 GiB de espacio disponibles

## Motor Docker

Se requiere Docker Engine versión 19 o posterior en el host antes de instalar el conector. ["Ver las instrucciones de instalación"](#)

## Instale el conector

Después de verificar que tiene un host Linux compatible, puede obtener el software Connector y luego instalarlo.

## Privilegios requeridos

Se requieren privilegios de usuario raíz para instalar el conector.

## Pasos

1. Compruebe que docker está activado y en ejecución.

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

2. Descargue el instalador del conector para redes restringidas sin acceso a Internet desde el ["Sitio de soporte de NetApp"](#)
3. Copie el instalador en el host Linux.
4. Asigne permisos para ejecutar el script.



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

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

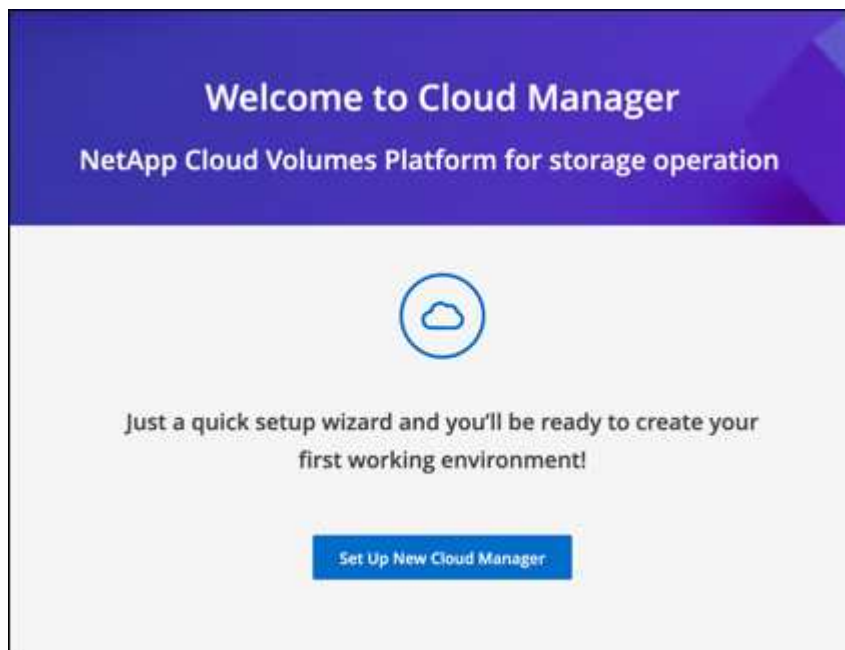
5. Ejecute el script de instalación:

```
sudo /path/Cloud-Manager-Connector-offline-<version>
```

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

6. Abra un explorador web e introduzca `https://ipaddress[]` Donde *ipaddress* es la dirección IP del host Linux.

Debe ver la siguiente pantalla.



7. Haga clic en **Configurar nuevo BlueXP** y siga las indicaciones para configurar el sistema.
  - **Detalles del sistema:** Introduzca un nombre para el conector y el nombre de su empresa.



- **Crear usuario administrador:** Cree el usuario administrador para el sistema.

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

- **Revisión:** Revise los detalles, acepte el acuerdo de licencia y haga clic en **Configurar**.

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

## Resultado

El conector ya está instalado y puede empezar a utilizar las funciones de BlueXP que están disponibles en una implementación de sitio oscuro.

## El futuro

En un entorno local:

- ["Detección de clústeres de ONTAP en las instalaciones"](#)
- ["Replique datos entre clústeres ONTAP en las instalaciones"](#)
- ["Realice backups de datos de volúmenes de ONTAP en las instalaciones en StorageGRID mediante Cloud Backup"](#)
- ["Analice datos de volúmenes de ONTAP en las instalaciones mediante Cloud Data Sense"](#)

En un entorno de cloud, puede hacerlo ["Ponga en marcha Cloud Volumes ONTAP"](#)

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

# Búsqueda del ID del sistema de un conector

Para ayudarle a comenzar, es posible que su representante de NetApp le solicite el ID de sistema para un conector. El ID se utiliza normalmente para licencias y solución de problemas.

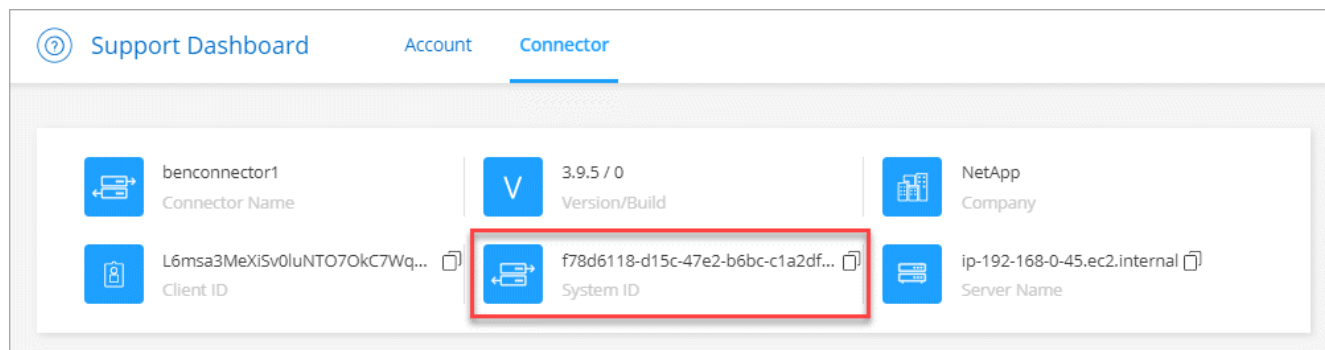
## Pasos

1. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda.

2. Haga clic en **Soporte > conector**.

El ID del sistema aparece en la parte superior.

**ejemplo**



## Gestión de conectores existentes

Después de crear uno o más conectores, puede gestionarlos cambiando entre conectores, conectándose a la interfaz de usuario local que se ejecuta en un conector, entre otros.

### 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. Haga clic en el menú desplegable **conector**, seleccione otro conector y, a continuación, haga clic en **conmutador**.



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

## Acceda a la interfaz de usuario local

Aunque debe realizar casi todas las tareas desde la interfaz de usuario de SaaS, todavía hay disponible una interfaz de usuario local en el conector. Si accede a BlueXP desde una región gubernamental o un sitio que no tiene acceso saliente a Internet, deberá utilizar la interfaz de usuario local que se ejecuta en el conector.

### 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. Introduzca su nombre de usuario y contraseña para iniciar sesión.

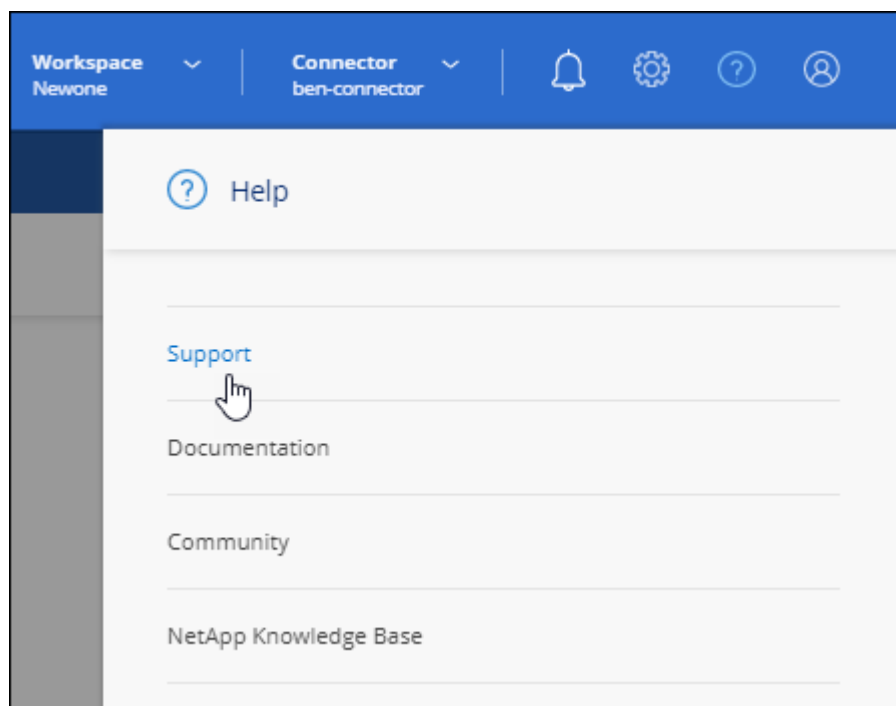
## Descargar o enviar un mensaje de AutoSupport

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.

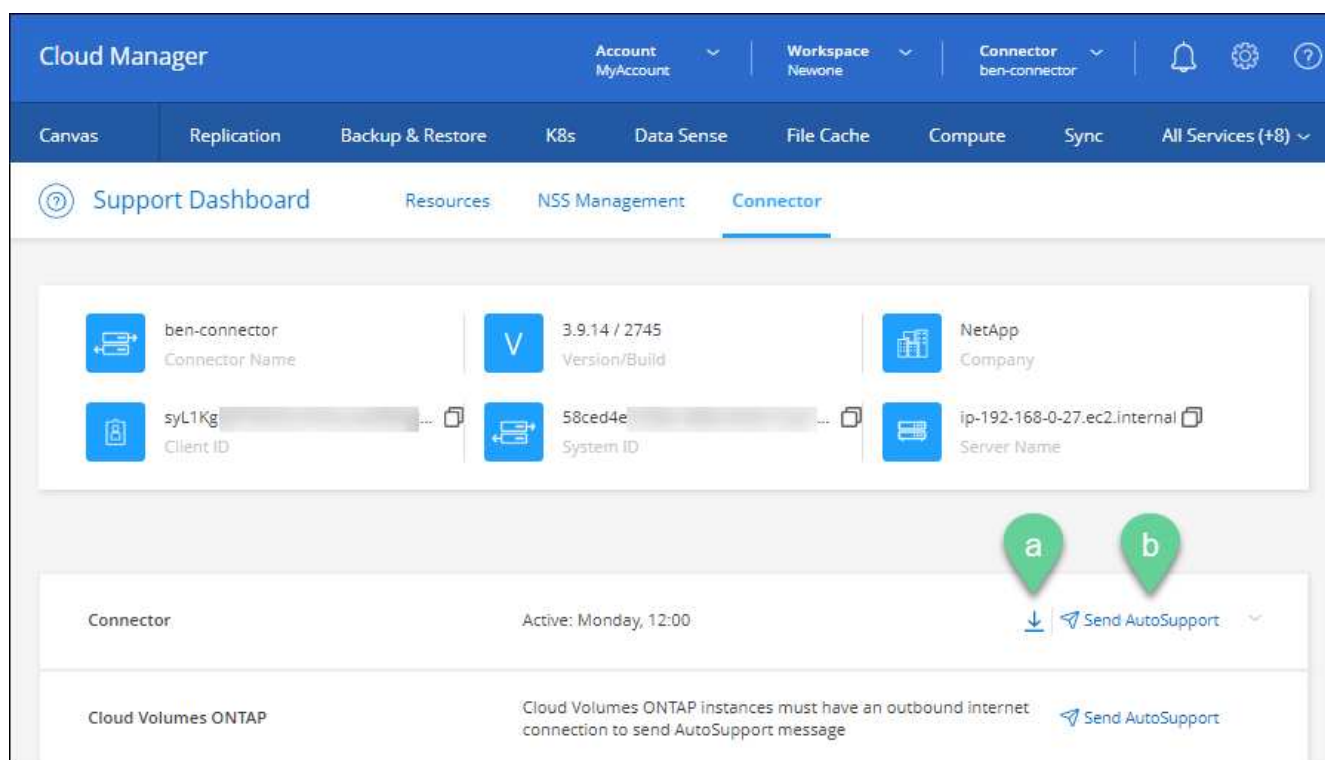
### Pasos

1. Conéctese a la interfaz de usuario local de Connector, como se describe en la sección anterior.

2. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Ayuda y seleccione **Soporte**.



3. Haga clic en **conector**.
4. En función de cómo necesite enviar la información al soporte de NetApp, seleccione una de las siguientes opciones:
- Seleccione la opción para descargar el mensaje de AutoSupport en el equipo local. Luego, puede enviarlo al soporte de NetApp mediante un método preferido.
  - Haga clic en **Enviar AutoSupport** para enviar directamente el mensaje al soporte de NetApp.



## 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.

["AWS Docs: Conéctese a su instancia de Linux"](#)

### Azure

Cuando creó el conector VM en Azure, eligió autenticarse con una contraseña o una 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"](#)

## Aplicar actualizaciones de seguridad

Actualice el sistema operativo en el conector para asegurarse de que se ha aplicado la revisión con las actualizaciones de seguridad más recientes.

### Pasos

1. Acceda al shell de la CLI en el host del conector.
2. Ejecute los siguientes comandos con privilegios elevados:

```
sudo -s
service netapp-service-manager stop
yum -y update --security
service netapp-service-manager start
```

## 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.
  - a. Ejecute el siguiente comando desde la interfaz de línea de comandos de Cloud Volumes ONTAP para quitar el destino de backup actual:

```
system configuration backup settings modify -destination ""
```

- b. Vaya a BlueXP y abra el entorno de trabajo.
- c. Haga clic en el menú y seleccione **Avanzado > copias de seguridad de configuración**.
- d. Haga clic en **establecer destino de copia de seguridad**.

## Editar los URI de un conector

Agregar y quitar los URI de un conector.

### Pasos

1. Haga clic en el menú desplegable **conector** del encabezado BlueXP.
2. Haga clic en **Administrar conectores**.
3. Haga clic en el menú de acción de un conector y haga clic en **Editar URI**.
4. Agregue y elimine URIs y, a continuación, haga clic en **aplicar**.

## 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"](#).

## Actualice el conector en una ubicación sin acceso a Internet

Si usted ["Se instaló el conector en una ubicación en la que no hay acceso a Internet"](#), Puede actualizar el conector cuando haya una versión más reciente disponible en el sitio de soporte de NetApp.

El conector debe reiniciarse durante el proceso de actualización para que la interfaz de usuario no esté disponible durante la actualización.

### Pasos

1. Descargue el software del conector de ["Sitio de soporte de NetApp"](#).
2. Copie el instalador en el host Linux.
3. Asigne permisos para ejecutar el script.

```
chmod +x /path/cloud-manager-connector-offline-<version>
```

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

4. Ejecute el script de instalación:

```
sudo /path/cloud-manager-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**.

### ¿Qué pasa con las actualizaciones de software en los hosts que tienen acceso a Internet?

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

## 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:

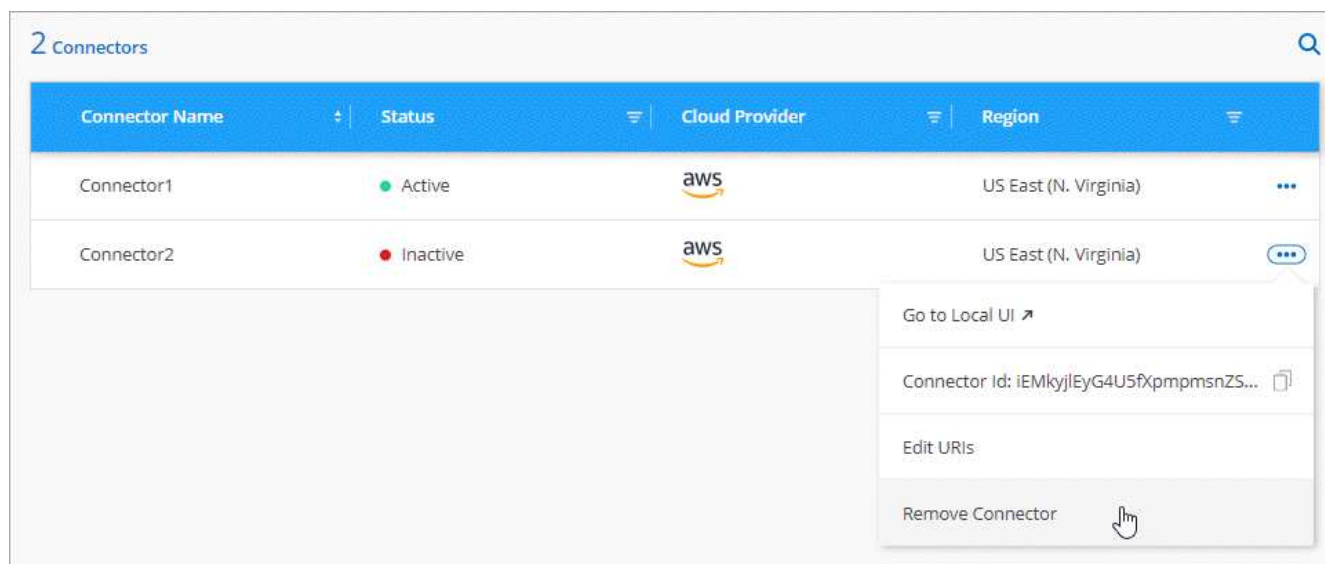
- Esta acción no elimina la máquina virtual.
- Esta acción no se puede revertir—una vez que se quita un conector de BlueXP, no se puede volver a agregar

### Pasos

1. Haga clic en el menú desplegable **conector** del encabezado BlueXP.
2. Haga clic en **Administrar conectores**.



3. Haga clic en el menú de acción de un conector inactivo y haga clic en **Quitar conector**.



4. Introduzca el nombre del conector que desea confirmar y, a continuación, haga clic en Quitar.

### Resultado

BlueXP quita el conector de sus registros.

## Desinstale el software del 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 de si ha instalado el conector en un host que tenga acceso a Internet o un host en una red restringida que no tenga acceso a Internet.

### Desinstale desde un host con acceso a Internet

El conector en línea incluye una secuencia de comandos de desinstalación que puede utilizar para desinstalar el software.

#### Paso

1. 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.

### Desinstale desde un host sin acceso a Internet

Use estos comandos si descargó el software del conector del sitio de soporte de NetApp y lo instaló en una red restringida que no tiene acceso a Internet.

#### Paso

1. Desde el host Linux, ejecute los siguientes comandos:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v  
rm -rf /opt/application/netapp/ds
```

## Gestión de un certificado HTTPS para un acceso seguro

De forma predeterminada, BlueXP utiliza un certificado autofirmado para el acceso HTTPS a la consola Web. Puede instalar un certificado firmado por una CA, que proporciona una mejor protección de seguridad que un certificado autofirmado.

### Antes de empezar

Debe crear un conector para poder cambiar la configuración de BlueXP. "[Vea cómo](#)".

### Instalar un certificado HTTPS

Instale un certificado firmado por una CA para obtener acceso seguro.

#### Pasos

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



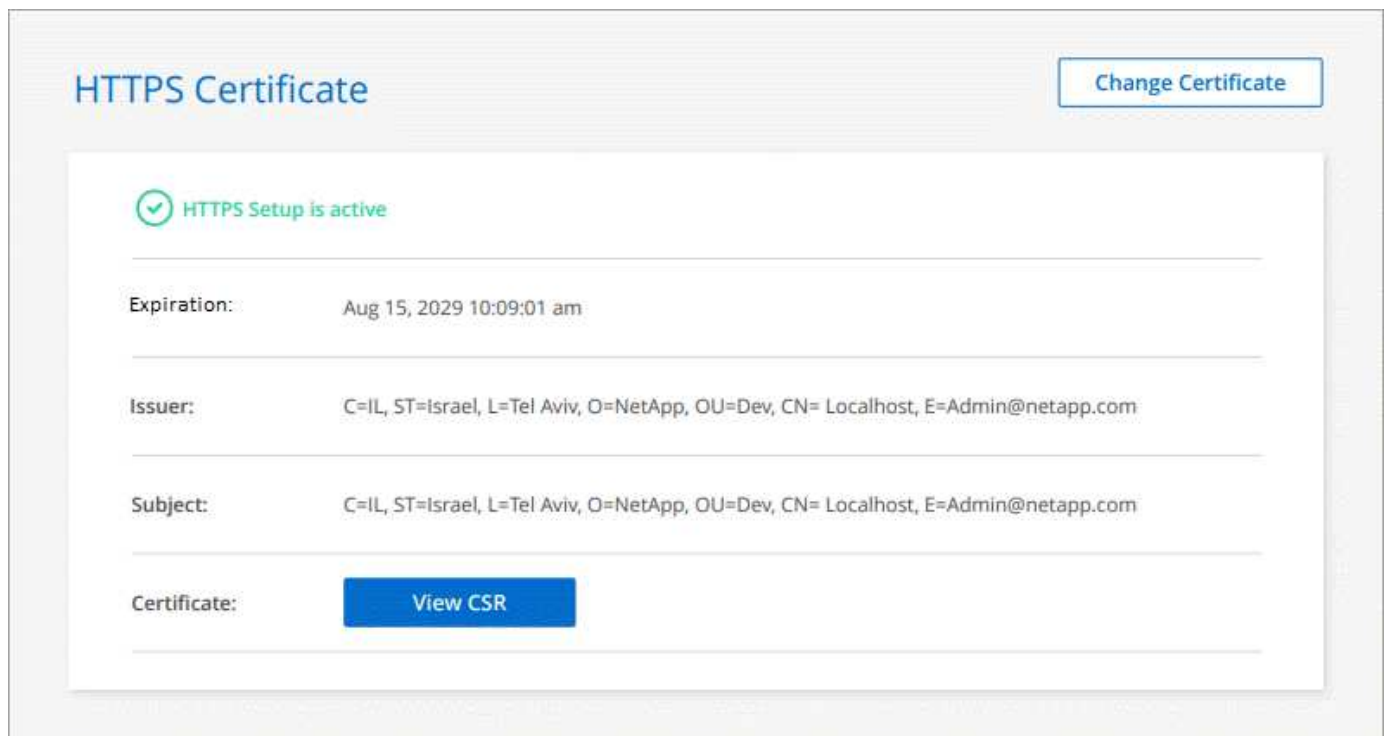
2. En la página HTTPS Setup, instale un certificado generando una solicitud de firma de certificación (CSR) o instalando su propio certificado firmado por una CA:

| Opción         | Descripción  |
|----------------|--|
| Genere una CSR | <p>a. Introduzca el nombre de host o DNS del host del conector (su nombre común) y, a continuación, haga clic en <b>generar CSR</b>.</p> <p>BlueXP muestra una solicitud de firma de certificado.</p> <p>b. Utilice la CSR para enviar una solicitud de certificado SSL a una CA.</p> <p>El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.</p> <p>c. Cargue el archivo de certificado y, a continuación, haga clic en <b>instalar</b>.</p> |

| Opción                                       | Descripción  |
|--|--|
| Instale su propio certificado firmado por CA | <p>a. Seleccione <b>instalar certificado firmado por CA</b>.</p> <p>b. Cargue el archivo de certificado y la clave privada y, a continuación, haga clic en <b>instalar</b>.</p> <p>El certificado debe utilizar el formato X.509 codificado con Privacy Enhanced Mail (PEM) base-64.</p> |

## Resultado

Ahora BlueXP utiliza el certificado firmado por CA para proporcionar acceso HTTPS seguro. La siguiente imagen muestra una cuenta de BlueXP configurada para un acceso seguro:



## Renovación del 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, haga clic en el icono Configuración y seleccione **Configuración HTTPS**.

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

2. Haga clic en **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.

BlueXP admite HTTP y HTTPS. El servidor proxy puede estar en la nube o en la red.

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.

### 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 realiza ninguna operación antes de continuar.

#### Pasos

1. ["Inicie sesión en la interfaz SaaS de BlueXP"](#) Desde un equipo que tiene una conexión de red a la instancia de conector.

Si el conector no tiene una dirección IP pública, necesitará una conexión VPN o deberá conectarse desde un host de salto que esté en la misma red que el conector.

2. Haga clic en el menú desplegable **conector** y, a continuación, haga clic en **Ir a la interfaz de usuario local** para ver un conector específico.



La interfaz BlueXP que se ejecuta en el conector se carga en una nueva pestaña del navegador.

3. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **Configuración del conector**.



4. En **General**, haga clic en **Configuración de proxy HTTP**.
5. Configure el proxy:
  - a. Haga clic en **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 se requiere autenticación básica para el servidor
  - d. Haga clic en **Guardar**.



BlueXP no admite contraseñas que incluyan el carácter @.

## 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. En la parte superior derecha de la consola de BlueXP, haga clic en el icono Configuración y seleccione **Configuración del conector**.



2. En **General**, haga clic en **Support Direct API Traffic**.
3. Haga clic en la casilla de verificación para activar la opción y, a continuación, haga clic en **Guardar**.

## Configuración predeterminada del conector

Es posible que desee obtener más información sobre el 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.xlarge.
- El sistema operativo de la imagen es Red Hat Enterprise Linux 7.6 (HVM).

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

- El nombre de usuario de la instancia de EC2 Linux es 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 DS3 v2.
- El sistema operativo de la imagen es CentOS 7.6.

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

- El disco del sistema predeterminado es un disco SSD premium de 100 GiB.

## Detalles de Google Cloud

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

- La instancia del equipo virtual es n2-standard-4.
- El sistema operativo de la imagen es Red Hat Enterprise Linux 8.6.

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

- 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 las imágenes de conector y Docker.

- `/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 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 acceso HTTPS



## Información de copyright

Copyright © 2023 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.