



# **Configure un conector**

## **Cloud Manager 3.8**

NetApp  
March 25, 2024

# Tabla de contenidos

- Configure un conector ..... 1
- Más información sobre conectores ..... 1
- Requisitos de red para el conector ..... 3
- Crear un conector en AWS desde Cloud Manager ..... 15
- Crear un conector en Azure desde Cloud Manager ..... 18
- Creación de un conector en GCP desde Cloud Manager ..... 20

# Configure un conector

## Más información sobre conectores

En la mayoría de los casos, un administrador de cuentas tendrá que poner en marcha un *Connector* en su red local o en la nube. El conector permite a Cloud Manager gestionar recursos y procesos dentro de su entorno de cloud público.

### Cuando se necesita un conector

Se requiere un conector para utilizar cualquiera de las siguientes funciones en Cloud Manager:

- Cloud Volumes ONTAP
- Clústeres de ONTAP en las instalaciones
- Cumplimiento de normativas en el cloud
- Kubernetes
- Backup a cloud
- Supervisión
- Organización en niveles en las instalaciones
- Caché de archivos global
- Detección de bloques de Amazon S3

Se requiere un conector **no** para Azure NetApp Files, Cloud Volumes Service o Cloud Sync.



Mientras que un conector no es necesario para configurar y administrar Azure NetApp Files, es necesario un conector si desea utilizar Cloud Compliance para analizar datos de Azure NetApp Files.

### Ubicaciones admitidas

Se admite un conector en las siguientes ubicaciones:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- En sus instalaciones



Si desea crear un sistema Cloud Volumes ONTAP en Google Cloud, también debe tener un conector en Google Cloud. No puede utilizar un conector que se ejecute en otra ubicación.

### Los conectores deben permanecer en funcionamiento

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

Por ejemplo, un conector es un componente clave en la salud y el funcionamiento de los sistemas de Cloud

Volumes ONTAP PAYGO. Si el conector está apagado, los sistemas de Cloud Volumes ONTAP PAYGO se apagarán tras perder la comunicación con un conector durante más de 14 días.

## Cómo crear un conector

Un administrador de cuentas debe crear un conector antes de que un administrador de área de trabajo pueda crear un entorno de trabajo Cloud Volumes ONTAP y utilizar cualquiera de las demás funciones enumeradas anteriormente.

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

- Directamente desde Cloud Manager (recomendado)
  - ["Cree en AWS"](#)
  - ["Cree en Azure"](#)
  - ["Crear en GCP"](#)
- ["Desde el AWS Marketplace"](#)
- ["Desde Azure Marketplace"](#)
- ["Descargando e instalando el software en un Linux existente host"](#)

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

## Permisos

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

### Permisos para crear un conector

El usuario que crea un conector desde Cloud Manager necesita permisos específicos para implementar la instancia en el proveedor de cloud que usted elija. Cloud Manager le recordará los requisitos de permisos al crear un conector.

["Vea políticas para cada proveedor de cloud"](#).

### Permisos para la instancia de conector

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

Al crear un conector directamente desde Cloud Manager, Cloud Manager crea el conector con los permisos que necesita. No hay nada que usted necesita hacer.

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

["Vea políticas para cada proveedor de cloud"](#).

## Cuándo usar varios conectores

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

A continuación, se muestran algunos ejemplos:

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

## Cuándo cambiar entre conectores

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

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

## La interfaz de usuario local

Mientras debe realizar casi todas las tareas de la ["Interfaz de usuario de SaaS"](#), una interfaz de usuario local todavía está disponible en el conector. Esta interfaz es necesaria para algunas tareas que se deben realizar desde el propio conector:

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

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

## Actualizaciones de conectores

El conector actualiza automáticamente su software a la última versión, siempre que lo haya hecho ["acceso a internet de salida"](#) para obtener la actualización de software.

## Requisitos de red para el conector

Configure su red de modo que Connector pueda gestionar recursos y procesos en su entorno de cloud público. El paso más importante es garantizar el acceso saliente a Internet a varios puntos finales.



Si la red utiliza un servidor proxy para toda la comunicación a Internet, puede especificar el servidor proxy en la página Configuración. Consulte ["Configuración del conector para utilizar un servidor proxy"](#).

## Conexión a redes de destino

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

Por ejemplo, si instala un conector en la red corporativa, debe configurar una conexión VPN al VPC o a vnet

en el que inicie Cloud Volumes ONTAP.

## Acceso a Internet de salida

El conector requiere acceso saliente a Internet para gestionar recursos y procesos dentro de su entorno de nube pública. El acceso saliente a Internet también es necesario si desea instalar manualmente el conector en un host Linux o acceder a la interfaz de usuario local que se ejecuta en el conector.

En las siguientes secciones se identifican los puntos finales específicos.

### Extremos para gestionar recursos en AWS

Un conector se pone en contacto con los siguientes extremos cuando se gestionan recursos en AWS:

Puntos finales	Específico
Servicios de AWS (amazonaws.com): <ul style="list-style-type: none"><li>• Formación CloudFormation</li><li>• Cloud computing elástico (EC2)</li><li>• Servicio de gestión de claves (KMS)</li><li>• Servicio de token de seguridad (STS)</li><li>• Simple Storage Service (S3)</li></ul> El extremo exacto depende de la región en la que se implemente Cloud Volumes ONTAP. <a href="#">"Consulte la documentación de AWS para obtener más detalles."</a>	Permite al conector poner en marcha y gestionar Cloud Volumes ONTAP en AWS.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	Solicitudes de API a Cloud Central de NetApp.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Proporciona acceso a imágenes, manifiestos y plantillas de software.
<a href="https://repo.cloud.support.netapp.com">https://repo.cloud.support.netapp.com</a>	Se utiliza para descargar las dependencias de Cloud Manager.
<a href="http://repo.mysql.com/">http://repo.mysql.com/</a>	Se utiliza para descargar MySQL.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Permite al conector acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Permite a NetApp transmitir datos desde registros de auditoría.

Puntos finales	Específico
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
<a href="https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist">https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist</a>	Se utiliza para añadir su ID de cuenta de AWS a la lista de usuarios permitidos para Backup en S3.
<a href="https://support.netapp.com/aods/asupmessage">https://support.netapp.com/aods/asupmessage</a> <a href="https://support.netapp.com/asupprod/post/1.0/postAsup">https://support.netapp.com/asupprod/post/1.0/postAsup</a>	Comunicación con AutoSupport de NetApp.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Permite a NetApp recopilar la información necesaria para resolver problemas de soporte.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
<p>Diversas ubicaciones de terceros, por ejemplo:</p> <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul> <p>Las ubicaciones de terceros están sujetas a cambios.</p>	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

### Extremos para gestionar recursos en Azure

Un conector se pone en contacto con los siguientes extremos al gestionar recursos en Azure:

Puntos finales	Específico
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en la mayoría de las regiones de Azure.
<a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a> <a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>	Permite que Cloud Manager ponga en marcha y gestione Cloud Volumes ONTAP en las regiones de Azure Alemania.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	Permite a Cloud Manager implementar y gestionar Cloud Volumes ONTAP en las regiones de Azure US Gov.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	Solicitudes de API a Cloud Central de NetApp.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Proporciona acceso a imágenes, manifiestos y plantillas de software.
<a href="https://repo.cloud.support.netapp.com">https://repo.cloud.support.netapp.com</a>	Se utiliza para descargar las dependencias de Cloud Manager.
<a href="http://repo.mysql.com/">http://repo.mysql.com/</a>	Se utiliza para descargar MySQL.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Permite al conector acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
<a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a>	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Permite a NetApp transmitir datos desde registros de auditoría.
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Comunicación con AutoSupport de NetApp.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Permite a NetApp recopilar la información necesaria para resolver problemas de soporte.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).



<b>Puntos finales</b>	<b>Específico</b>
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
*.blob.core.windows.net	Necesario para pares de alta disponibilidad cuando se utiliza un proxy.
Diversas ubicaciones de terceros, por ejemplo: <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul> Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

## Extremos para gestionar recursos en GCP

Un conector se pone en contacto con los siguientes extremos al gestionar recursos en GCP:

<b>Puntos finales</b>	<b>Específico</b>
<a href="https://www.googleapis.com">https://www.googleapis.com</a>	Permite que el conector se ponga en contacto con las API de Google para poner en marcha y gestionar Cloud Volumes ONTAP en GCP.
<a href="https://api.services.cloud.netapp.com:443">https://api.services.cloud.netapp.com:443</a>	Solicitudes de API a Cloud Central de NetApp.
<a href="https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com">https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com</a>	Proporciona acceso a imágenes, manifiestos y plantillas de software.
<a href="https://repo.cloud.support.netapp.com">https://repo.cloud.support.netapp.com</a>	Se utiliza para descargar las dependencias de Cloud Manager.
<a href="http://repo.mysql.com/">http://repo.mysql.com/</a>	Se utiliza para descargar MySQL.
<a href="https://cognito-idp.us-east-1.amazonaws.com">https://cognito-idp.us-east-1.amazonaws.com</a> <a href="https://cognito-identity.us-east-1.amazonaws.com">https://cognito-identity.us-east-1.amazonaws.com</a> <a href="https://sts.amazonaws.com">https://sts.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.amazonaws.com</a>	Permite al conector acceder y descargar manifiestos, plantillas e imágenes de actualización de Cloud Volumes ONTAP.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a>	Acceso a imágenes de software de componentes de contenedor para una infraestructura que ejecuta Docker y proporciona una solución para las integraciones de servicios con Cloud Manager.
<a href="https://kinesis.us-east-1.amazonaws.com">https://kinesis.us-east-1.amazonaws.com</a>	Permite a NetApp transmitir datos desde registros de auditoría.

Puntos finales	Específico
<a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Comunicación con el servicio Cloud Manager, que incluye cuentas de Cloud Central.
<a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a>	Comunicación con Cloud Central de NetApp para la autenticación de usuario centralizada.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	Comunicación con AutoSupport de NetApp.
<a href="https://support.netapp.com/svcgw">https://support.netapp.com/svcgw</a> <a href="https://support.netapp.com/ServiceGW/entitlement">https://support.netapp.com/ServiceGW/entitlement</a> <a href="https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com">https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com</a>	Comunicación con NetApp para la licencia del sistema y el registro de soporte.
<a href="https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com">https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com</a> <a href="https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com">https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com</a> <a href="https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com">https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com</a>	Permite a NetApp recopilar la información necesaria para resolver problemas de soporte.
<a href="https://ipa-signer.cloudmanager.netapp.com">https://ipa-signer.cloudmanager.netapp.com</a>	Permite que Cloud Manager genere licencias (por ejemplo, una licencia de FlexCache para Cloud Volumes ONTAP).
<a href="https://packages.cloud.google.com/yum">https://packages.cloud.google.com/yum</a> <a href="https://github.com/NetApp/trident/releases/download/">https://github.com/NetApp/trident/releases/download/</a>	Necesario para conectar los sistemas Cloud Volumes ONTAP con un clúster de Kubernetes. Los extremos permiten la instalación de Trident de NetApp.
Diversas ubicaciones de terceros, por ejemplo: <ul style="list-style-type: none"> <li>• <a href="https://repo1.maven.org/maven2">https://repo1.maven.org/maven2</a></li> <li>• <a href="https://oss.sonatype.org/content/repositories">https://oss.sonatype.org/content/repositories</a></li> <li>• <a href="https://repo.typesafe.com">https://repo.typesafe.com</a></li> </ul> Las ubicaciones de terceros están sujetas a cambios.	Durante las actualizaciones, Cloud Manager descarga los paquetes más recientes para dependencias de terceros.

## Extremos para instalar el conector en un host Linux

Tiene la opción de instalar manualmente el software Connector en su propio host Linux. Si lo hace, el instalador del conector debe acceder a las siguientes direcciones URL durante el proceso de instalación:

- <http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm>
- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>
- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>

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 a los que se accede desde el explorador Web cuando se utiliza el local UI

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. La máquina que ejecuta el explorador Web debe tener conexiones con los siguientes puntos finales:

Puntos finales	Específico
El host del conector	<p>Debe introducir la dirección IP del host desde un explorador web para cargar la consola de Cloud Manager.</p> <p>Según su conectividad con el proveedor de cloud, puede usar la IP privada o una IP pública asignada al host:</p> <ul style="list-style-type: none"><li>• Una IP privada funciona si dispone de una VPN y acceso directo a la red virtual</li><li>• Una IP pública funciona en cualquier situación de red</li></ul> <p>En cualquier caso, debe proteger el acceso a la red garantizando que las reglas de grupo de seguridad permiten el acceso sólo desde IP o subredes autorizadas.</p>
<a href="https://auth0.com">https://auth0.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	El explorador web se conecta con estos extremos para conseguir una autenticación de usuario centralizada mediante NetApp Cloud Central.
<a href="https://widget.intercom.io">https://widget.intercom.io</a>	Si busca un chat integrado en los productos que le permita hablar con expertos en cloud de NetApp.

## Puertos y grupos de seguridad

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

### Reglas para el conector en AWS

El grupo de seguridad del conector requiere reglas entrantes y salientes.

#### Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local Interfaz de usuario y conexiones desde Cloud Compliance
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

Protocolo	Puerto	Específico
TCP	3128	Proporciona a la instancia de Cloud Compliance acceso a Internet si la red AWS no utiliza NAT o proxy

### Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

### Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

### Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

<b>Servicio</b>	<b>Protocolo</b>	<b>Puerto</b>	<b>Destino</b>	<b>Específico</b>
Active Directory	TCP	88	Bosque de Active Directory	Autenticación Kerberos V.
	TCP	139	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP	389	Bosque de Active Directory	LDAP
	TCP	445	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	TCP	749	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	UDP	137	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Bosque de Active Directory	Servicio de datagramas NetBIOS
	UDP	464	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
	TCP	8088	Backup en S3	Llamadas API a Backup en S3
DNS	UDP	53	DNS	Utilizado para resolver DNS por Cloud Manager
Cumplimiento de normativas en el cloud	HTTP	80	Instancia de cumplimiento de normativas cloud	Cumplimiento de normativas cloud para Cloud Volumes ONTAP

## Reglas para Conector en Azure

El grupo de seguridad del conector requiere reglas entrantes y salientes.

### Reglas de entrada

El origen de las reglas entrantes en el grupo de seguridad predefinido es 0.0.0.0/0.

Puerto	Protocolo	Específico
22	SSH	Proporciona acceso SSH al host de Conector
80	HTTP	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
443	HTTPS	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

### Reglas de salida

El grupo de seguridad predefinido para el conector abre todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

### Reglas de salida básicas

El grupo de seguridad predefinido para el conector incluye las siguientes reglas de salida.

Puerto	Protocolo	Específico
Todo	Todos los TCP	Todo el tráfico saliente
Todo	Todas las UDP	Todo el tráfico saliente

### Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.

<b>Servicio</b>	<b>Puerto</b>	<b>Protocolo</b>	<b>Destino</b>	<b>Específico</b>
Active Directory	88	TCP	Bosque de Active Directory	Autenticación Kerberos V.
	139	TCP	Bosque de Active Directory	Sesión de servicio NetBIOS
	389	TCP	Bosque de Active Directory	LDAP
	445	TCP	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	464	TCP	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	749	TCP	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	137	UDP	Bosque de Active Directory	Servicio de nombres NetBIOS
	138	UDP	Bosque de Active Directory	Servicio de datagramas NetBIOS
	464	UDP	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	443	HTTPS	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a AWS y ONTAP y envía mensajes de AutoSupport a NetApp
Llamadas API	3000	TCP	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
DNS	53	UDP	DNS	Utilizado para resolver DNS por Cloud Manager

### Reglas para el conector en GCP

Las reglas de firewall para el conector requieren reglas de entrada y salida.

#### Reglas de entrada

El origen de las reglas de entrada en las reglas de firewall predefinidas es 0.0.0.0/0.

Protocolo	Puerto	Específico
SSH	22	Proporciona acceso SSH al host de Connector
HTTP	80	Proporciona acceso HTTP desde navegadores web de cliente al local interfaz de usuario
HTTPS	443	Proporciona acceso HTTPS desde exploradores web de cliente al local interfaz de usuario

### Reglas de salida

Las reglas de firewall predefinidas para el conector abren todo el tráfico saliente. Si eso es aceptable, siga las reglas básicas de la salida. Si necesita más reglas rígidas, utilice las reglas avanzadas de salida.

### Reglas de salida básicas

Las reglas de firewall predefinidas para el conector incluyen las siguientes reglas de salida.

Protocolo	Puerto	Específico
Todos los TCP	Todo	Todo el tráfico saliente
Todas las UDP	Todo	Todo el tráfico saliente

### Reglas salientes avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir sólo los puertos necesarios para la comunicación saliente por parte del conector.



La dirección IP de origen es el host del conector.



Servicio	Protocolo	Puerto	Destino	Específico
Active Directory	TCP	88	Bosque de Active Directory	Autenticación Kerberos V.
	TCP	139	Bosque de Active Directory	Sesión de servicio NetBIOS
	TCP	389	Bosque de Active Directory	LDAP
	TCP	445	Bosque de Active Directory	Microsoft SMB/CIFS sobre TCP con trama NetBIOS
	TCP	464	Bosque de Active Directory	Kerberos V cambiar y establecer contraseña (SET_CHANGE)
	TCP	749	Bosque de Active Directory	Contraseña de modificación y definición de Kerberos V de Active Directory (RPCSEC_GSS)
	UDP	137	Bosque de Active Directory	Servicio de nombres NetBIOS
	UDP	138	Bosque de Active Directory	Servicio de datagramas NetBIOS
	UDP	464	Bosque de Active Directory	Administración de claves Kerberos
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres de ONTAP y Internet saliente	API llama a GCP y ONTAP, y envía mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	LIF de gestión de clústeres de ONTAP	Llamadas API a ONTAP
DNS	UDP	53	DNS	Utilizado para resolver DNS por Cloud Manager

## Crear un conector en AWS desde Cloud Manager

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

En esta página se describe cómo crear un conector en AWS directamente desde Cloud Manager. También tiene la opción a. "[Cree el conector desde el AWS Marketplace](#)", o. "[descargue el software e instálelo en su propio host](#)".

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



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

## Configuración de permisos de AWS para crear un conector

Antes de poder implementar un conector desde Cloud Manager, debe asegurarse de que su cuenta de AWS tenga los permisos correctos.

### Pasos

1. Descargue la política del IAM del conector desde la siguiente ubicación:

["NetApp Cloud Manager: Políticas de AWS, Azure y GCP"](#)

2. Desde la consola del IAM de AWS, cree su propia política copiando y pegando el texto de la política IAM del conector.
3. Adjunte la política que creó en el paso anterior al usuario IAM que creará el conector desde Cloud Manager.

### Resultado

El usuario de AWS ahora tiene los permisos necesarios para crear el conector desde Cloud Manager. Deberá especificar las claves de acceso de AWS para este usuario cuando se le solicite Cloud Manager.

## Creación de un conector en AWS

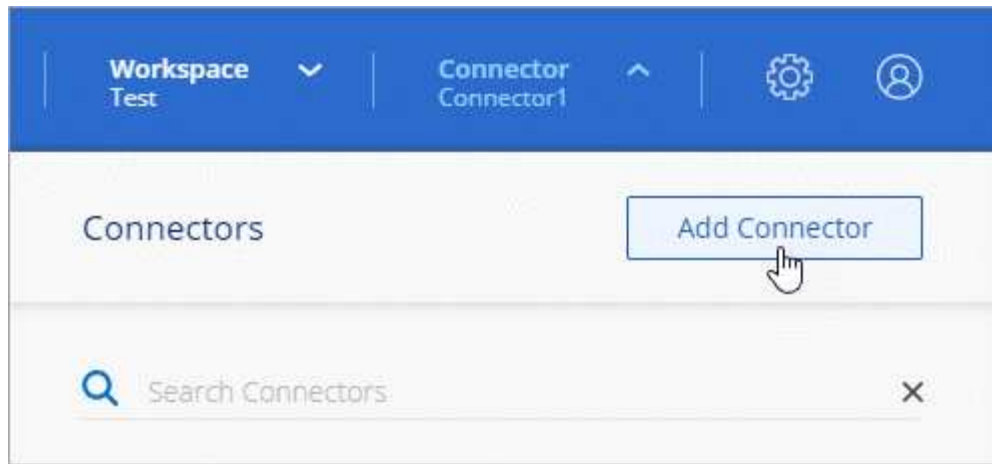
Cloud Manager permite crear un conector en AWS directamente desde su interfaz de usuario.

### Lo que necesitará

- Una clave secreta y de acceso AWS para un IAM usuario que tiene la "[permisos necesarios](#)".
- Un VPC, una subred y un teclados en la región de AWS que usted elija.

### Pasos

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



2. Haga clic en **Iniciar**.
3. Elija **Amazon Web Services** como su proveedor de cloud.

Recuerde que el conector debe tener una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que está planeando habilitar.

["Obtenga más información sobre los requisitos de red del conector"](#).

4. Revise lo que necesitará y haga clic en **continuar**.
5. Proporcione la información necesaria:
  - **credenciales de AWS:** Introduzca un nombre para la instancia y especifique la clave de acceso y la clave secreta de AWS que cumplan los requisitos de permisos.
  - **ubicación:** Especifique una región, VPC y subred de AWS para la instancia.
  - **Red:** Seleccione el par de claves que se va a utilizar con la instancia, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
  - **Grupo de seguridad:** Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.



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

6. Haga clic en **Crear**.

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

### Después de terminar

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

# Crear un conector en Azure desde Cloud Manager

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

En esta página se describe cómo crear un conector en Azure directamente desde Cloud Manager. También tiene la opción a. "[Cree el conector desde Azure Marketplace](#)", o. "[descargue el software e instálelo en su propio host](#)".

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



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

## Configurar permisos de Azure para crear un conector

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

### Pasos

1. Cree un rol personalizado con la política de Azure para Connector:
  - a. Descargue el "[Política de Azure para Connector](#)".



Haga clic con el botón derecho del ratón en el enlace y haga clic en **Guardar enlace como...** para descargar el archivo.

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

### ejemplo

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

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

El ejemplo siguiente muestra cómo crear una función personalizada con la CLI de Azure 2.0:

```
az role definition create --role-definition  
C:\Policy_for_Setup_As_Service_Azure.json
```

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

2. Asigne el rol al usuario que implementará Connector desde Cloud Manager:
  - a. Abra el servicio **Suscripciones** y seleccione la suscripción del usuario.

- b. Haga clic en **Control de acceso (IAM)**.
- c. Haga clic en **Agregar > Agregar asignación de rol** y, a continuación, agregue los permisos:
  - Seleccione el rol **Azure SetupAsService**.



Azure SetupAsService es el nombre predeterminado que se proporciona en "[Política de implementación de conectores para Azure](#)". Si seleccionó otro nombre para el rol, seleccione ese nombre.

- Asigne acceso a un usuario, grupo o aplicación **AD de Azure**.
- Seleccione la cuenta de usuario.
- Haga clic en **Guardar**.

### Resultado

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

## Creación de un conector en Azure

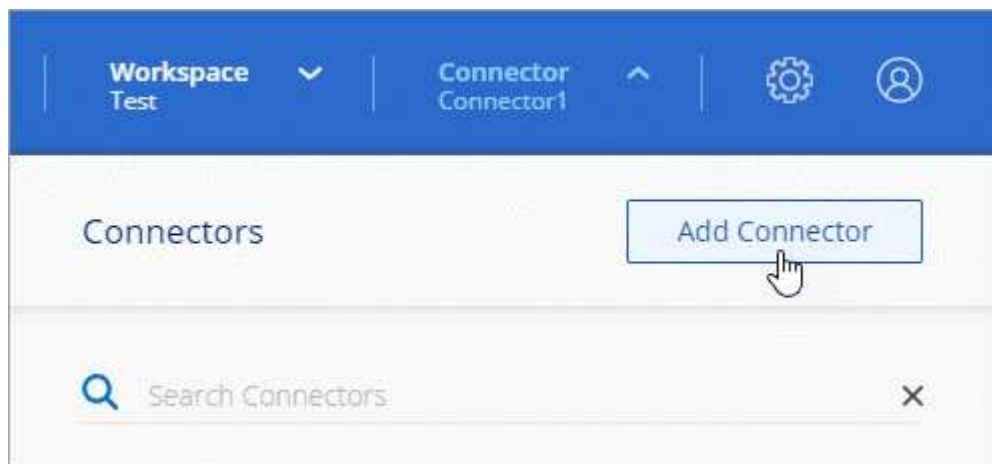
Cloud Manager permite crear un conector en Azure directamente desde su interfaz de usuario.

### Lo que necesitará

- La "[permisos necesarios](#)" Para su cuenta de Azure.
- Una suscripción a Azure.
- Una red virtual y una subred en su región de Azure preferida.

### Pasos

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



2. Haga clic en **Iniciar**.
3. Elija **Microsoft Azure** como proveedor de cloud.

Recuerde que el conector debe tener una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que está planeando habilitar.

["Obtenga más información sobre los requisitos de red del conector"](#).

4. Revise lo que necesitará y haga clic en **continuar**.
5. Si se le solicita, inicie sesión en su cuenta de Microsoft, que debería tener los permisos necesarios para crear la máquina virtual.

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



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

6. Proporcione la información necesaria:
  - **autenticación de VM:** Introduzca un nombre para la máquina virtual y un nombre de usuario y contraseña o clave pública.
  - **Configuración básica:** Elija una suscripción a Azure, una región de Azure y si desea crear un nuevo grupo de recursos o utilizar un grupo de recursos existente.
  - **Red:** Elija un vnet y una subred, si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
  - **Grupo de seguridad:** Elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita el acceso entrante HTTP, HTTPS y SSH.



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

7. Haga clic en **Crear**.

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

### Después de terminar

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

## Creación de un conector en GCP desde Cloud Manager

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

En esta página se describe cómo crear un conector en GCP directamente desde Cloud Manager. También tiene la opción a. "[descargue el software e instálelo en su propio host](#)".

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



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

## Configuración de los permisos de GCP para crear un conector

Antes de poder implementar un conector desde Cloud Manager, debe asegurarse de que su cuenta de GCP tiene los permisos correctos y de que se haya configurado una cuenta de servicio para la máquina virtual Connector.

### Pasos

1. Compruebe que el usuario de GCP que implementa Cloud Manager desde NetApp Cloud Central tiene los permisos en el ["Política de implementación de conectores para GCP"](#).

["Puede crear una función personalizada con el archivo YAML"](#) y, a continuación, adjuntarlo al usuario. Deberá utilizar la línea de comandos gcloud para crear la función.

2. Configure una cuenta de servicio con los permisos que Cloud Manager necesita para crear y gestionar sistemas Cloud Volumes ONTAP en los proyectos.

Asociará esta cuenta de servicio con Connector VM al crearla desde Cloud Manager.

- a. ["Crear un rol en GCP"](#) esto incluye los permisos definidos en la ["Política de Cloud Manager para GCP"](#). De nuevo, deberá utilizar la línea de comandos gcloud.

Los permisos contenidos en este archivo YAML son diferentes a los del paso 2a.

- b. ["Cree una cuenta de servicio de GCP y aplique el rol personalizado que acaba de crear"](#).
- c. Si desea poner en marcha Cloud Volumes ONTAP en otros proyectos, ["Conceda el acceso añadiendo la cuenta de servicio con la nube La función de gerente de ese proyecto"](#). Deberá repetir este paso con cada proyecto.

### Resultado

El usuario GCP ahora tiene los permisos necesarios para crear el conector desde Cloud Manager y se configura la cuenta de servicio para el conector VM.

## Habilitar las API de Google Cloud

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

### Paso

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

## Creación de un conector en GCP

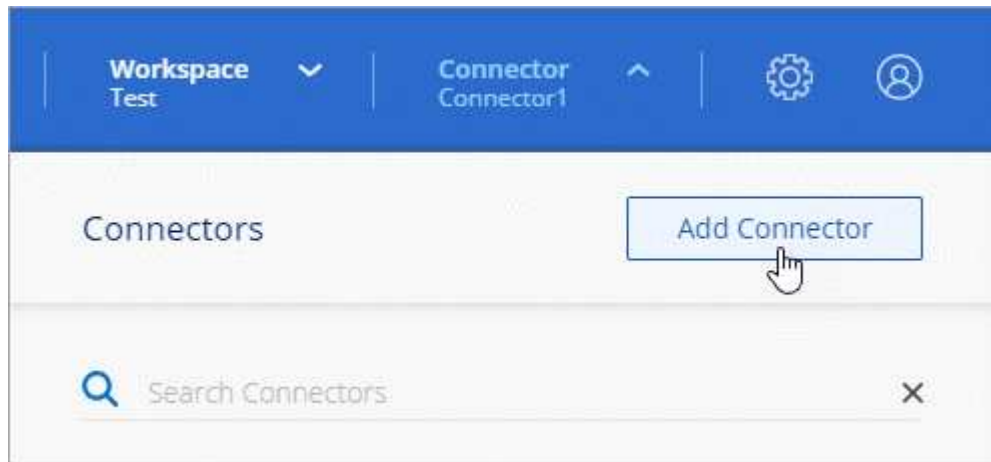
Cloud Manager le permite crear un conector en GCP directamente desde su interfaz de usuario.

## Lo que necesitará

- La "[permisos necesarios](#)" Para su cuenta de Google Cloud.
- Un proyecto de Google Cloud.
- Cuenta de servicio con los permisos necesarios para crear y gestionar Cloud Volumes ONTAP.
- VPC y una subred en la región de su elección de Google Cloud.

## Pasos

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



2. Haga clic en **Iniciar**.
3. Elija **Google Cloud Platform** como su proveedor de cloud.

Recuerde que el conector debe tener una conexión de red al tipo de entorno de trabajo que está creando y a los servicios que está planeando habilitar.

["Obtenga más información sobre los requisitos de red del conector"](#).

4. Revise lo que necesitará y haga clic en **continuar**.
5. 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.

6. Proporcione la información necesaria:
  - **Configuración básica:** Escriba un nombre para la instancia de la máquina virtual y especifique un proyecto y una cuenta de servicio que tenga los permisos necesarios.
  - **ubicación:** Especifique una región, zona, VPC y subred para la instancia.
  - **Red:** Elija si desea activar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.
  - **Directiva de firewall:** Elija si desea crear una nueva directiva de firewall o si desea seleccionar una directiva de firewall existente que permita el acceso entrante HTTP, HTTPS y SSH.





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

7. Haga clic en **Crear**.

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

#### **Después de terminar**

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

## Información de copyright

Copyright © 2024 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.