



Introducción a NetApp Console (modo restringido)

NetApp Console setup and administration

NetApp

February 09, 2026

Tabla de contenidos

Introducción a NetApp Console (modo restringido)	1
Flujo de trabajo de introducción (modo restringido)	1
Prepárese para la implementación en modo restringido	1
Paso 1: Comprenda cómo funciona el modo restringido	1
Paso 2: Revisar las opciones de instalación	2
Paso 3: Revisar los requisitos del host	2
Paso 4: Instalar Podman o Docker Engine	5
Paso 5: Preparar el acceso a la red	8
Paso 6: Preparar los permisos de la nube	13
Paso 7: Habilitar las API de Google Cloud	22
Implementar el agente de consola en modo restringido	23
Paso 1: Instalar el agente de la consola	23
Paso 2: Configurar la NetApp Console	31
Paso 3: Proporcionar permisos al agente de la consola	32
Suscribirse a NetApp Intelligent Services (modo restringido)	35
Qué puedes hacer a continuación (modo restringido)	41

Introducción a NetApp Console (modo restringido)

Flujo de trabajo de introducción (modo restringido)

Comience a utilizar la NetApp Console en modo restringido preparando su entorno e implementando el agente de la consola.

El modo restringido generalmente lo utilizan los gobiernos estatales y locales y las empresas reguladas, incluidas las implementaciones en las regiones de AWS GovCloud y Azure Government. Antes de comenzar, asegúrese de comprender "[Agentes de consola](#)" y "[modos de implementación](#)".

1

"Prepárese para el despliegue"

1. Prepare un host Linux dedicado que cumpla con los requisitos de CPU, RAM, espacio en disco, herramienta de orquestación de contenedores y más.
2. Configurar redes que proporcionen acceso a las redes de destino, acceso a Internet saliente para instalaciones manuales e Internet saliente para acceso diario.
3. Configure permisos en su proveedor de nube para que pueda asociar esos permisos con la instancia del agente de consola después de implementarla.

2

"Implementar el agente de consola"

1. Instale el agente de consola desde el marketplace de su proveedor de nube o instalando manualmente el software en su propio host Linux.
2. Configure la NetApp Console abriendo un navegador web e ingresando la dirección IP del host Linux.
3. Proporcione al agente de la consola los permisos que configuró previamente.

3

"Suscríbete a los NetApp Intelligent Services (opcional)"

Opcional: Suscríbase a NetApp Intelligent Services desde el mercado de su proveedor de nube para pagar los servicios de datos a una tarifa por hora (PAYGO) o mediante un contrato anual. Los NetApp Intelligent Services incluyen NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience y NetApp Disaster Recovery. La NetApp Data Classification está incluida en su suscripción sin costo adicional.

Prepárese para la implementación en modo restringido

Prepare su entorno antes de implementar NetApp Console en modo restringido. Debe revisar los requisitos del host, preparar la red, configurar permisos y más.

Paso 1: Comprenda cómo funciona el modo restringido

Comprenda cómo funciona la NetApp Console en modo restringido antes de comenzar.

Utilice la interfaz basada en navegador disponible localmente desde el agente de NetApp Console instalado.

No se puede acceder a la NetApp Console desde la consola basada en web que se proporciona a través de la capa SaaS.

Además, no todas las funciones de la consola y los servicios de datos de NetApp están disponibles.

["Aprenda cómo funciona el modo restringido"](#) .

Paso 2: Revisar las opciones de instalación

En el modo restringido, solo puedes instalar el agente de consola en la nube. Están disponibles las siguientes opciones de instalación:

- Desde AWS Marketplace
- Desde Azure Marketplace
- Instalación manual del agente de consola en su propio host Linux que se ejecuta en AWS, Azure o Google Cloud

Paso 3: Revisar los requisitos del host

Un host debe cumplir requisitos específicos de sistema operativo, RAM y puerto para ejecutar el agente de consola.

Cuando implementa el agente de consola desde AWS o Azure Marketplace, la imagen incluye los componentes de software y sistema operativo necesarios. Simplemente tienes que elegir un tipo de instancia que cumpla con los requisitos de CPU y RAM.

Host dedicado

El agente de consola requiere un host dedicado. Se admite cualquier arquitectura si cumple estos requisitos de tamaño:

- CPU: 8 núcleos u 8 vCPU
- RAM: 32 GB
- Espacio en disco: se recomiendan 165 GB para el host, con los siguientes requisitos de partición:
 - /opt: Debe haber 120 GiB de espacio disponibles

El agente utiliza /opt Para instalar el /opt/application/netapp directorio y su contenido.

- /var: Debe haber 40 GiB de espacio disponibles

El agente de consola requiere este espacio en /var porque Podman o Docker están diseñados para crear los contenedores dentro de este directorio. En concreto, crearán contenedores en el /var/lib/containers/storage directorio y /var/lib/docker para Docker. Los montajes externos o enlaces simbólicos no funcionan para este espacio.

Tipo de instancia de AWS EC2

Un tipo de instancia que cumple con los requisitos de CPU y RAM. NetApp recomienda t3.2xlarge.

Tamaño de la máquina virtual de Azure

Un tipo de instancia que cumple con los requisitos de CPU y RAM. NetApp recomienda Standard_D8s_v3.

Tipo de máquina de Google Cloud

Un tipo de instancia que cumple con los requisitos de CPU y RAM. NetApp recomienda n2-standard-8.

El agente de consola es compatible con Google Cloud en una instancia de máquina virtual con un sistema operativo compatible. ["Características de las máquinas virtuales protegidas"](#)

Hipervisor

Se requiere un hipervisor alojado o de metal desnudo que esté certificado para ejecutar un sistema operativo compatible.

Requisitos del sistema operativo y del contenedor

El agente de consola es compatible con los siguientes sistemas operativos cuando se utiliza la consola en modo estándar o modo restringido. Se requiere una herramienta de orquestación de contenedores antes de instalar el agente.

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux		<p>9,6</p> <ul style="list-style-type: none">• Sólo versiones en idioma inglés.• El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación del agente.	4.0.0 o posterior con la consola en modo estándar o modo restringido	<p>Podman versión 5.4.0 con podman-compose 1.5.0.</p> <p>Ver los requisitos de configuración de Podman .</p>

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Compatible con modo de aplicación o modo permisivo		<p>9.1 a 9.4</p> <ul style="list-style-type: none"> • Sólo versiones en idioma inglés. • El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación del agente. 	3.9.50 o posterior con la consola en modo estándar o modo restringido	<p>Podman versión 4.9.4 con podman-compose 1.5.0.</p> <p>Ver los requisitos de configuración de Podman .</p>
Compatible con modo de aplicación o modo permisivo		<p>8.6 a 8.10</p> <ul style="list-style-type: none"> • Sólo versiones en idioma inglés. • El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación del agente. 	3.9.50 o posterior con la consola en modo estándar o modo restringido	<p>Podman versión 4.6.1 o 4.9.4 con podman-compose 1.0.6.</p> <p>Ver los requisitos de configuración de Podman .</p>

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Compatible con modo de aplicación o modo permisivo	Ubuntu		24.04 LTS	3.9.45 o posterior con la NetApp Console en modo estándar o modo restringido
Motor Docker 23.06 a 28.0.0.	No compatible		22.04 LTS	3.9.50 o posterior

Paso 4: Instalar Podman o Docker Engine

Para instalar manualmente el agente de consola, prepare el host instalando Podman o Docker Engine.

Dependiendo de su sistema operativo, se requiere Podman o Docker Engine antes de instalar el agente.

- Podman es necesario para Red Hat Enterprise Linux 8 y 9.

[Ver las versiones compatibles de Podman .](#)

- Se requiere Docker Engine para Ubuntu.

[Ver las versiones compatibles de Docker Engine .](#)

Ejemplo 1. Pasos

Podman

Siga estos pasos para instalar y configurar Podman:

- Habilitar e iniciar el servicio podman.socket
- Instalar Python3
- Instalar el paquete podman-compose versión 1.0.6
- Agregue podman-compose a la variable de entorno PATH
- Si usa Red Hat Enterprise Linux, verifique que su versión de Podman esté usando Netavark Aardvark DNS en lugar de CNI



Ajuste el puerto aardvark-dns (predeterminado: 53) después de instalar el agente para evitar conflictos en el puerto DNS. Siga las instrucciones para configurar el puerto.

Pasos

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

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

2. Instalar Podman.

Puede obtener Podman desde los repositorios oficiales de Red Hat Enterprise Linux.

- a. Para Red Hat Enterprise Linux 9,6:

```
sudo dnf install podman-5:<version>
```

Donde <versión> es la versión compatible de Podman que estás instalando. [Ver las versiones compatibles de Podman](#).

- b. Para Red Hat Enterprise Linux 9.1 a 9.4:

```
sudo dnf install podman-4:<version>
```

Donde <versión> es la versión compatible de Podman que estás instalando. [Ver las versiones compatibles de Podman](#).

- c. Para Red Hat Enterprise Linux 8:

```
sudo dnf install podman-4:<version>
```

Donde <versión> es la versión compatible de Podman que estás instalando. [Ver las versiones compatibles de Podman](#).

3. Habilite e inicie el servicio podman.socket.

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

4. Instalar python3.

```
sudo dnf install python3
```

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

Este paso es necesario porque podman-compose está disponible en el repositorio de Paquetes adicionales para Enterprise Linux (EPEL).

6. Si utiliza Red Hat Enterprise 9:

a. Instalar el paquete del repositorio EPEL.

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

+

a. Instalar el paquete podman-compose 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Si utiliza Red Hat Enterprise Linux 8:

a. Instalar el paquete del repositorio EPEL.

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

b. Instalar el paquete podman-compose 1.0.6.

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



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

c. Si usa Red Hat Enterprise Linux 8, verifique que su versión de Podman esté usando NetAvark con Aardvark DNS en lugar de CNI.

i. Verifique si su networkBackend está configurado en CNI ejecutando el siguiente comando:

```
podman info | grep networkBackend
```

ii. Si la red Backend está configurada en CNI , tendrás que cambiarlo a netavark .

iii. Instalar netavark y aardvark-dns utilizando el siguiente comando:

```
dnf install aardvark-dns netavark
```

iv. Abrir el /etc/containers/containers.conf archivo y modificar la opción network_backend para usar "netavark" en lugar de "cni".

Si /etc/containers/containers.conf no existe, realice los cambios de configuración a /usr/share/containers/containers.conf .

v. Reiniciar podman.

```
systemctl restart podman
```

vi. Confirme que networkBackend ahora se cambió a "netavark" usando el siguiente comando:

```
podman info | grep networkBackend
```

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. ["Ver instrucciones de instalación desde Docker"](#)

Siga los pasos para instalar una versión compatible de Docker Engine. No instale la última versión, ya que la consola no es compatible.

2. Verifique que Docker esté habilitado y ejecutándose.

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

Paso 5: Preparar el acceso a la red

Configure el acceso a la red para que el agente de la consola pueda administrar recursos en su nube pública. Además de tener una red virtual y una subred para el agente de consola, debe asegurarse de que se cumplan los siguientes requisitos.

Conexiones a redes de destino

Asegúrese de que el agente de la consola tenga una conexión de red a las ubicaciones de almacenamiento. Por ejemplo, la VPC o VNet donde planea implementar Cloud Volumes ONTAP, o el centro de datos donde residen sus clústeres ONTAP locales.

Preparar la red para el acceso de los usuarios a la NetApp Console

En el modo restringido, los usuarios acceden a la consola desde la máquina virtual del agente de consola. El agente de la consola se comunica con algunos puntos finales para completar tareas de administración de datos. Estos puntos finales se contactan desde la computadora de un usuario cuando se completan acciones específicas desde la Consola.

 Los agentes de consola anteriores a la versión 4.0.0 necesitan puntos finales adicionales. Si actualizó a 4.0.0 o posterior, puede eliminar los puntos finales antiguos de su lista de permitidos. ["Obtenga más información sobre el acceso a la red necesario para versiones anteriores a 4.0.0."](#)

+

Puntos finales	Objetivo
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Proporcionar funciones y servicios dentro de la NetApp Console.
\ https://cdn.auth0.com \ https://services.cloud.netapp.com	Su navegador web se conecta a estos puntos finales para la autenticación centralizada de usuarios a través de la NetApp Console.

Acceso a Internet saliente para operaciones diarias

La ubicación de red del agente de la consola debe tener acceso a Internet saliente. Debe poder acceder a los servicios SaaS de la NetApp Console , así como a los puntos finales dentro de su respectivo entorno de nube pública.

Puntos finales	Objetivo
Entornos AWS	<p>Servicios de AWS (amazonaws.com):</p> <ul style="list-style-type: none"> • Formación de nubes • Nube de cómputo elástica (EC2) • Gestión de identidad y acceso (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Servicio de almacenamiento simple (S3)
Para administrar los recursos de AWS. El punto final depende de su región de AWS. "Consulte la documentación de AWS para obtener más detalles."	<p>Amazon FsX para NetApp ONTAP:</p> <ul style="list-style-type: none"> • api.workloads.netapp.com
La consola basada en web se comunica con este punto final para interactuar con las API de Workload Factory para administrar y operar FSx para cargas de trabajo basadas en ONTAP .	Entornos Azure
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para administrar recursos en regiones públicas de Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Para administrar recursos en regiones de Azure Government.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para administrar recursos en las regiones de Azure China.

Puntos finales	Objetivo
Entornos de Google Cloud	\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects
Para administrar recursos en Google Cloud.	*Puntos finales de la NetApp Console *
\ https://mysupport.netapp.com	Para obtener información de licencias y enviar mensajes de AutoSupport al soporte de NetApp .
\ https://signin.b2c.netapp.com	Para actualizar las credenciales del sitio de soporte de NetApp (NSS) o para agregar nuevas credenciales de NSS a la NetApp Console.
\ https://support.netapp.com	Para obtener información de licencias y enviar mensajes de AutoSupport al soporte de NetApp , así como para recibir actualizaciones de software para Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Proporcionar funciones y servicios dentro de la NetApp Console.

Puntos finales	Objetivo
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	<p>Para obtener imágenes para las actualizaciones del agente de consola.</p> <ul style="list-style-type: none"> • Cuando se implementa un nuevo agente, la verificación de validación prueba la conectividad con los puntos finales actuales. Si utilizas "puntos finales anteriores", la comprobación de validación falla. Para evitar este error, omita la comprobación de validación. <p>Aunque los puntos finales anteriores aún son compatibles, NetApp recomienda actualizar las reglas de firewall a los puntos finales actuales lo antes posible. "Aprenda a actualizar su lista de puntos finales".</p> <ul style="list-style-type: none"> • Cuando actualice los puntos finales actuales en su firewall, sus agentes existentes continuarán funcionando.

Dirección IP pública en Azure

Si desea utilizar una dirección IP pública con la máquina virtual del agente de consola en Azure, la dirección IP debe usar una SKU básica para garantizar que la consola use esta dirección IP pública.

The screenshot shows the 'Create public IP address' dialog box. It has the following fields:

- Name ***: A text input field containing "newIP".
- SKU ***: A dropdown menu with two options: "Basic" (selected) and "Standard".
- Assignment**: A dropdown menu with two options: "Dynamic" (unchecked) and "Static" (selected).

Si utiliza una dirección IP de SKU estándar, la consola utiliza la dirección IP *privada* del agente de la consola, en lugar de la IP pública. Si la máquina que estás usando para acceder a la consola no tiene acceso a esa dirección IP privada, las acciones desde la consola fallarán.

Servidor proxy

NetApp admite configuraciones de proxy explícitas y transparentes. Si está utilizando un proxy transparente, solo necesita proporcionar el certificado para el servidor proxy. Si está utilizando un proxy explícito, también necesitará la dirección IP y las credenciales.

- Dirección IP
- Cartas credenciales
- Certificado HTTPS

Puertos

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

- HTTP (80) y HTTPS (443) brindan acceso a la interfaz de usuario local, que utilizará en circunstancias excepcionales.
- SSH (22) solo es necesario si necesita conectarse al host para solucionar problemas.
- Se requieren conexiones entrantes a través del puerto 3128 si implementa sistemas Cloud Volumes ONTAP en una subred donde no hay una conexión a Internet saliente disponible.

Si los sistemas Cloud Volumes ONTAP no tienen una conexión a Internet saliente para enviar mensajes de AutoSupport , la consola configura automáticamente esos sistemas para usar un servidor proxy que está incluido con el agente de la consola. El único requisito es garantizar que el grupo de seguridad del agente de la consola permita conexiones entrantes a través del puerto 3128. Necesitará abrir este puerto después de implementar el agente de consola.

Habilitar NTP

Si planea utilizar NetApp Data Classification para escanear sus fuentes de datos corporativos, debe habilitar un servicio de Protocolo de tiempo de red (NTP) tanto en el agente de consola como en el sistema de NetApp Data Classification para que la hora se sincronice entre los sistemas. ["Obtenga más información sobre la clasificación de datos de NetApp"](#)

Si planea crear un agente de consola desde el mercado de su proveedor de nube, implemente este requisito de red después de crear el agente de consola.

Paso 6: Preparar los permisos de la nube

El agente de consola requiere permisos de su proveedor de nube para implementar Cloud Volumes ONTAP en una red virtual y utilizar los servicios de datos de NetApp . Debe configurar permisos en su proveedor de nube y luego asociar esos permisos con el agente de la consola.

Para ver los pasos necesarios, elija la opción de autenticación que desea utilizar para su proveedor de nube.

Rol de AWS IAM

Utilice una función de IAM para proporcionar permisos al agente de la consola.

Si está creando el agente de consola desde AWS Marketplace, se le solicitará que seleccione esa función de IAM cuando inicie la instancia EC2.

Si está instalando manualmente el agente de consola en su propio host Linux, adjunte el rol a la instancia EC2.

Pasos

1. Inicie sesión en la consola de AWS y navegue hasta el servicio IAM.
2. Crear una política:
 - a. Seleccione **Políticas > Crear política**.
 - b. Seleccione **JSON** y copie y pegue el contenido del "["Política de IAM para el agente de consola"](#)" .
 - c. Complete los pasos restantes para crear la política.
3. Crear un rol de IAM:
 - a. Seleccione **Roles > Crear rol**.
 - b. Seleccione **Servicio AWS > EC2**.
 - c. Agregue permisos adjuntando la política que acaba de crear.
 - d. Complete los pasos restantes para crear el rol.

Resultado

Ahora tiene un rol de IAM para la instancia EC2 del agente de consola.

Clave de acceso de AWS

Configurar permisos y una clave de acceso para un usuario de IAM. Necesitará proporcionar a la consola la clave de acceso de AWS después de instalar el agente de la consola y configurar la consola.

Pasos

1. Inicie sesión en la consola de AWS y navegue hasta el servicio IAM.
2. Crear una política:
 - a. Seleccione **Políticas > Crear política**.
 - b. Seleccione **JSON** y copie y pegue el contenido del "["Política de IAM para el agente de consola"](#)" .
 - c. Complete los pasos restantes para crear la política.

Según los servicios de datos de NetApp que planee utilizar, es posible que deba crear una segunda política.

Para las regiones estándar, los permisos se distribuyen en dos políticas. Se requieren dos políticas debido a un límite máximo de tamaño de caracteres para las políticas administradas en AWS.

["Obtenga más información sobre las políticas de IAM para el agente de consola"](#) .

3. Adjuntar las políticas a un usuario de IAM.
 - ["Documentación de AWS: Creación de roles de IAM"](#)
 - ["Documentación de AWS: Cómo agregar y eliminar políticas de IAM"](#)

4. Asegúrese de que el usuario tenga una clave de acceso que pueda agregar a la NetApp Console después de instalar el agente de la consola.

Rol de Azure

Cree un rol personalizado de Azure con los permisos necesarios. Asignarás esta función a la máquina virtual del agente de consola.

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

Pasos

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

["Documentación de Microsoft Azure: Configurar identidades administradas para recursos de Azure en una máquina virtual mediante el portal de Azure"](#)

2. Copiar el contenido del "[Permisos de roles personalizados para el Conector](#)" y guardarlos en un archivo JSON.
3. Modifique el archivo JSON agregando identificadores de suscripción de Azure al ámbito assignable.

Debe agregar el ID de cada suscripción de Azure que desee utilizar con la NetApp Console.

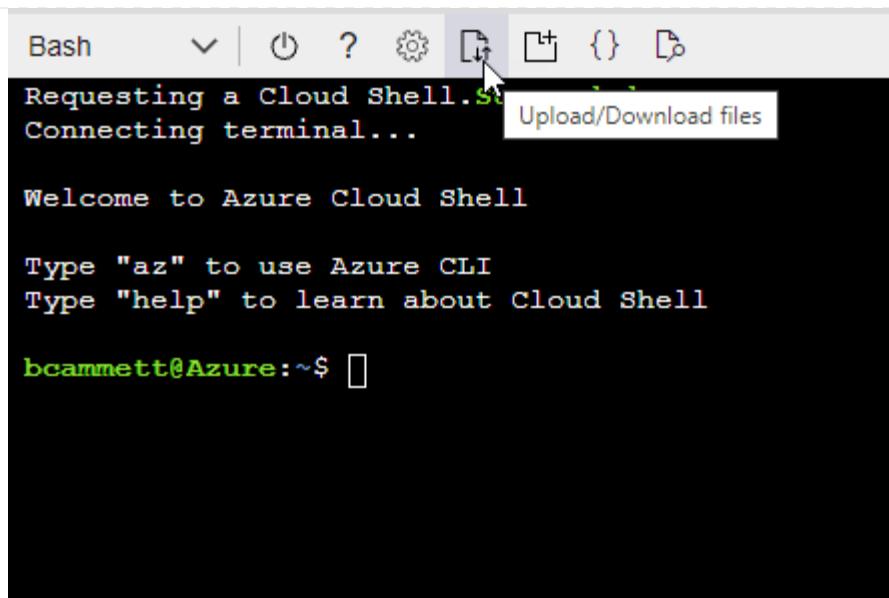
Ejemplo

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"  
]
```

4. Utilice el archivo JSON para crear un rol personalizado en Azure.

Los siguientes pasos describen cómo crear el rol mediante Bash en Azure Cloud Shell.

- a. Comenzar "[Azure Cloud Shell](#)" y elija el entorno Bash.
- b. Sube el archivo JSON.



- c. Utilice la CLI de Azure para crear el rol personalizado:

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

entidad de servicio de Azure

Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita la consola. Debe proporcionar a la consola estas credenciales después de instalar el agente de la consola.

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

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

Para más detalles, consulte "["Documentación de Microsoft Azure: Permisos necesarios"](#)

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

A screenshot of the Microsoft Azure portal. The top navigation bar shows "Microsoft Azure" and a search bar with "entra" typed in. Below the search bar, there are tabs: "All", "Services (24)", "Resources (10)", "Resource Groups (12)", and "Marketplace". Under the "Services" tab, there is a list of services. One service, "Microsoft Entra ID (1)", is highlighted with a red box and has a cursor pointing at it. Other services listed include "Central service instances for SAP solutions" and another "Microsoft Entra ID" service.

3. En el menú, seleccione **Registros de aplicaciones**.
4. Seleccione **Nuevo registro**.

5. Especifique detalles sobre la aplicación:

- **Nombre:** Ingrese un nombre para la aplicación.
- **Tipo de cuenta:** seleccione un tipo de cuenta (cualquiera funcionará con la NetApp Console).
- **URI de redirección:** Puede dejar este campo en blanco.

6. Seleccione **Registrarse**.

Ha creado la aplicación AD y la entidad principal de servicio.

Asignar la aplicación a un rol

1. Crear un rol personalizado:

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

- a. Copiar el contenido del "[Permisos de roles personalizados para el agente de la consola](#)" y guardarlos en un archivo JSON.
- b. Modifique el archivo JSON agregando identificadores de suscripción de Azure al ámbito assignable.

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

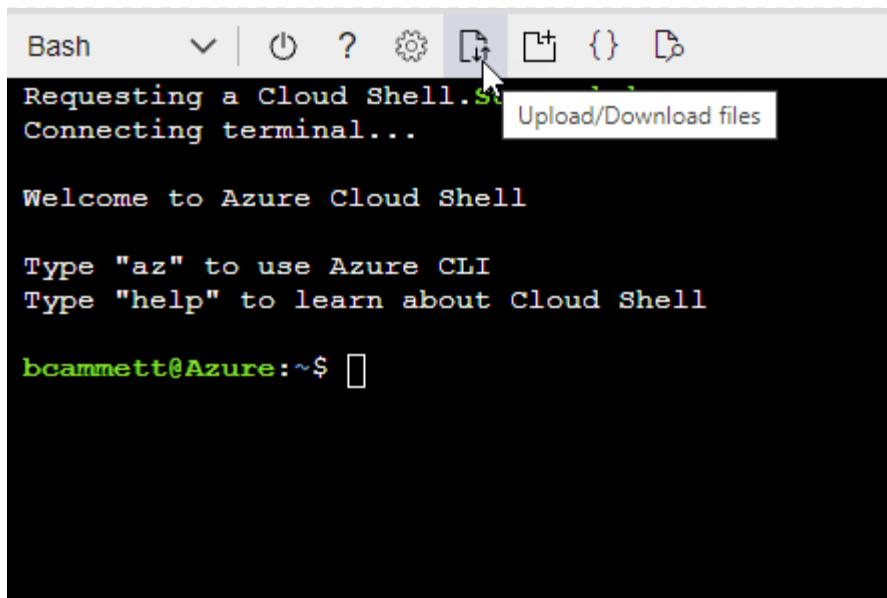
Ejemplo

```
"AssignableScopes": [  
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz",  
    "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzz",  
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"  
]
```

- c. Utilice el archivo JSON para crear un rol personalizado en Azure.

Los siguientes pasos describen cómo crear el rol mediante Bash en Azure Cloud Shell.

- Comenzar "[Azure Cloud Shell](#)" y elija el entorno Bash.
- Sube el archivo JSON.



- Utilice la CLI de Azure para crear el rol personalizado:

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

Ahora debería tener un rol personalizado llamado Operador de consola que puede asignar a la máquina virtual del agente de consola.

2. Asignar la aplicación al rol:

- Desde el portal de Azure, abra el servicio **Suscripciones**.
- Seleccione la suscripción.
- Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de rol**.
- En la pestaña **Rol**, seleccione el rol **Operador de consola** y seleccione **Siguiente**.
- En la pestaña **Miembros**, complete los siguientes pasos:
 - Mantenga seleccionado **Usuario, grupo o entidad de servicio**.
 - Seleccionar **Seleccionar miembros**.

Add role assignment

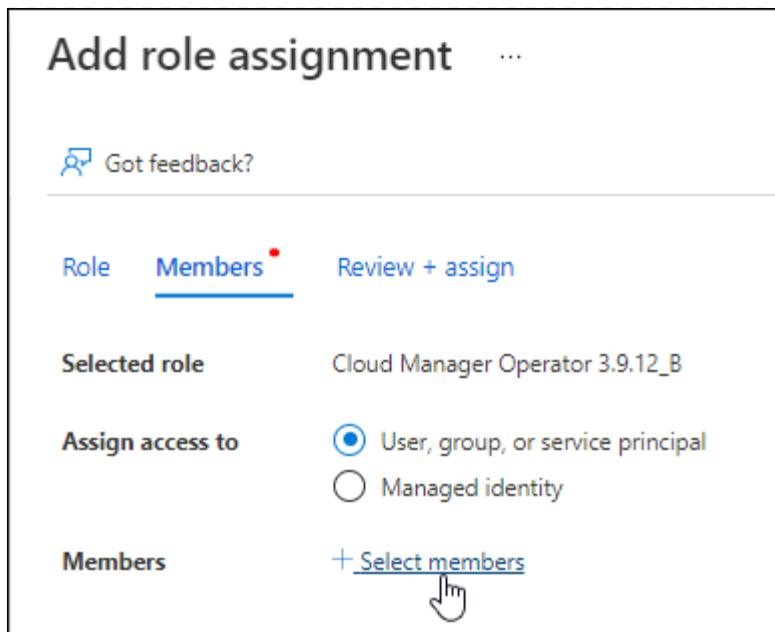
Got feedback?

Role **Members** * Review + assign

Selected role Cloud Manager Operator 3.9.12_B

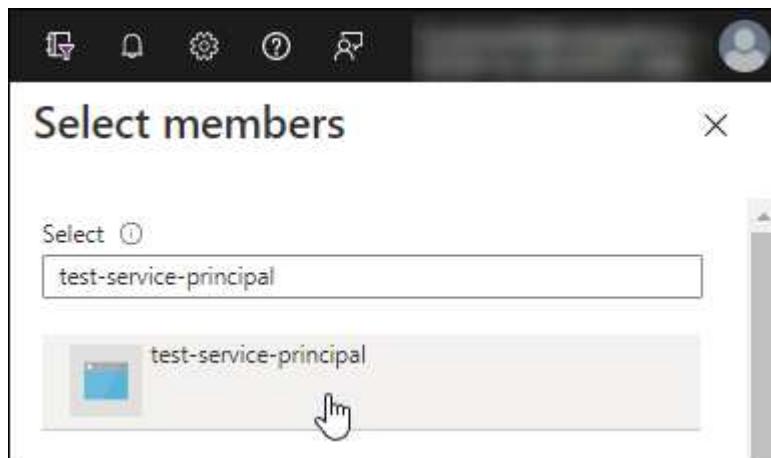
Assign access to User, group, or service principal Managed identity

Members [+ Select members](#)



- Busque el nombre de la aplicación.

He aquí un ejemplo:



- Seleccione la aplicación y seleccione **Seleccionar**.
 - Seleccione **Siguiente**.
- f. Seleccione **Revisar + asignar**.

La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

Si desea implementar Cloud Volumes ONTAP desde varias suscripciones de Azure, debe vincular la entidad de servicio a cada una de esas suscripciones. En la NetApp Console, puede seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

Agregar permisos de la API de administración de servicios de Windows Azure

1. En el servicio **Microsoft Entra ID**, seleccione **Registros de aplicaciones** y seleccione la aplicación.
2. Seleccione **Permisos de API > Agregar un permiso**.

3. En **API de Microsoft**, seleccione **Administración de servicios de Azure**.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.

Request API permissions

[All APIs](#)

Azure Service Management
<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search		PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation	Access Azure Service Management as organization users (preview)	Details	

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

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

The screenshot shows the Microsoft Entra ID App Registrations page. It displays a registration for an application named "test-service-principal". The "Display name" is "test-service-principal". The "Object ID" is "b37489a9-379f-49c2-b27c-e630514106a5". Two specific fields are highlighted with a red box: "Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3" and "Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a".

Cuando agrega la cuenta de Azure a la consola, debe proporcionar el identificador de la aplicación (cliente) y el identificador del directorio (inquilino) para la aplicación. La consola utiliza los ID para iniciar sesión mediante programación.

Crear un secreto de cliente

1. Abra el servicio **Microsoft Entra ID**.
2. Selecciona **Registros de aplicaciones** y selecciona tu aplicación.
3. Selecciona **Certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Selecciona **Agregar**.
6. Copia el valor del secreto del cliente.

>

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

			Copy to clipboard
DESCRIPTION	EXPIRES	VALUE	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRv4NLfdAcY7:+0vA	

Resultado

Su entidad de servicio ya está configurada y debería haber copiado el ID de la aplicación (cliente), el ID del directorio (inquilino) y el valor del secreto del cliente. Debe ingresar esta información en la consola cuando agregue una cuenta de Azure.

Cuenta de servicio de Google Cloud

Crea un rol y aplícalo a una cuenta de servicio que usarás para la instancia de VM del agente de consola.

Pasos

1. Crear un rol personalizado en Google Cloud:

- a. Cree un archivo YAML que incluya los permisos definidos en el "[Política del agente de consola para Google Cloud](#)" .
- b. Desde Google Cloud, activa Cloud Shell.
- c. Cargue el archivo YAML que incluye los permisos necesarios para el agente de consola.
- d. Cree un rol personalizado mediante el uso de `gcloud iam roles create dominio`.

El siguiente ejemplo crea un rol llamado "agente" a nivel de proyecto:

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

+

["Documentación de Google Cloud: Creación y administración de roles personalizados"](#)

2. Crear una cuenta de servicio en Google Cloud:

- a. Desde el servicio IAM y administración, seleccione **Cuentas de servicio > Crear cuenta de servicio**.
- b. Ingrese los detalles de la cuenta de servicio y seleccione **Crear y continuar**.
- c. Seleccione el rol que acaba de crear.
- d. Complete los pasos restantes para crear el rol.

["Documentación de Google Cloud: Creación de una cuenta de servicio"](#)

Paso 7: Habilitar las API de Google Cloud

Se requieren varias API para implementar Cloud Volumes ONTAP en Google Cloud.

Paso

1. "Habilite las siguientes API de Google Cloud en su proyecto"

- API de Cloud Deployment Manager V2
- API de Cloud Infrastructure Manager
- API de registro en la nube
- API del administrador de recursos en la nube
- API de Compute Engine
- API de gestión de identidad y acceso (IAM)
- API del servicio de gestión de claves en la nube (KMS) (necesaria solo si planeas usar NetApp Backup and Recovery con claves de cifrado gestionadas por el cliente (CMEK))
- API de Cloud Quotas (necesaria para implementaciones de Cloud Volumes ONTAP usando Infrastructure Manager)

Implementar el agente de consola en modo restringido

Implemente el agente de consola en modo restringido para poder usar la NetApp Console con conectividad saliente limitada. Para comenzar, instale el agente de la consola, configúrelo accediendo a la interfaz de usuario que se ejecuta en el agente de la consola y luego proporcione los permisos de nube que configuró previamente.

Paso 1: Instalar el agente de la consola

Instale el agente de consola desde el marketplace de su proveedor de nube o manualmente en un host Linux.

Debes tener preparado tu entorno antes de instalar el agente de consola. Puede instalarlo desde AWS Marketplace, desde Azure Marketplace o manualmente en su propio host Linux que se ejecute en AWS, Azure o Google Cloud.

Mercado comercial de AWS

Antes de empezar

Tenga lo siguiente:

- Una VPC y una subred que cumple con los requisitos de red.

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

- Una función de IAM con una política adjunta que incluye los permisos necesarios para el agente de la consola.

["Aprenda a configurar los permisos de AWS"](#)

- Permisos para suscribirse y cancelar la suscripción a AWS Marketplace para su usuario de IAM.
- Una comprensión de los requisitos de CPU y RAM para el agente.

["Requisitos del agente de revisión".](#)

- Un par de claves para la instancia EC2.

Pasos

1. Ir a la ["Listado de agentes de la NetApp Console en AWS Marketplace"](#)

2. En la página de Marketplace, seleccione **Continuar con la suscripción**.

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

El proceso de suscripción puede tardar unos minutos.

4. Una vez completado el proceso de suscripción, seleccione **Continuar a la configuración**.

5. En la página **Configurar este software**, asegúrese de haber seleccionado la región correcta y luego seleccione **Continuar con el inicio**.

6. En la página **Iniciar este software**, en **Elegir acción**, seleccione **Iniciar a través de EC2** y luego seleccione **Iniciar**.

Utilice la consola EC2 para iniciar la instancia y adjuntar una función de IAM. Esto no es posible con la acción **Iniciar desde sitio web**.

7. Siga las instrucciones para configurar e implementar la instancia:

- **Nombre y etiquetas:** Ingrese un nombre y etiquetas para la instancia.
- **Imágenes de aplicaciones y sistema operativo:** omitir esta sección. La AMI del agente de consola ya está seleccionada.
- **Tipo de instancia:** según la disponibilidad de la región, elija un tipo de instancia que cumpla con los requisitos de RAM y CPU (t3.2xlarge está preseleccionado y se recomienda).
- **Par de claves (inicio de sesión):** seleccione el par de claves que desea utilizar para conectarse de forma segura a la instancia.
- **Configuración de red:** edite la configuración de red según sea necesario:
 - Elija la VPC y la subred deseadas.
 - Especifique si la instancia debe tener una dirección IP pública.

- Especifique la configuración del grupo de seguridad que habilite los métodos de conexión necesarios para la instancia del agente de consola: SSH, HTTP y HTTPS.

["Ver las reglas del grupo de seguridad para AWS"](#) .

- **Configurar almacenamiento:** mantenga el tamaño y el tipo de disco predeterminados para el volumen raíz.

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

- **Detalles avanzados:** en **Perfil de instancia de IAM**, elija el rol de IAM que incluye los permisos necesarios para el agente de consola.

- **Resumen:** Revise el resumen y seleccione **Iniciar instancia**.

Resultado

AWS inicia el software con la configuración especificada. El agente de consola se implementa en aproximadamente cinco minutos.

¿Que sigue?

Configurar la NetApp Console.

Mercado gubernamental de AWS

Antes de empezar

Tenga lo siguiente:

- Una VPC y una subred que cumple con los requisitos de red.

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

- Una función de IAM con una política adjunta que incluye los permisos necesarios para el agente de la consola.

["Aprenda a configurar los permisos de AWS"](#)

- Permisos para suscribirse y cancelar la suscripción a AWS Marketplace para su usuario de IAM.
- Un par de claves para la instancia EC2.

Pasos

1. Vaya a la oferta del agente de NetApp Console en AWS Marketplace.
 - a. Abra el servicio EC2 y seleccione **Iniciar instancia**.
 - b. Seleccione **AWS Marketplace**.
 - c. Busque NetApp Console y seleccione la oferta.

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

Bluexp

BlueXP - Manual Installation without access keys

NetApp

★★★★★ (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.

Select

More info

- d. Seleccione **Continuar**.
2. Siga las instrucciones para configurar e iniciar la instancia:
- **Elija un tipo de instancia:** según la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.2xlarge).
 - ["Revisar los requisitos de la instancia"](#) .
 - **Configurar detalles de la instancia:** seleccione una 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 con sus requisitos.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2 VPC4QA (default)	<input type="button" value="Create new VPC"/>
Subnet	subnet-39536c13 QASubnet1 us-east-1b	<input type="button" value="Create new subnet"/> 155 IP Addresses available
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<input type="button" value="Create new Capacity Reservation"/>
IAM role	Cloud_Manager	<input type="button" value="Create new IAM role"/>
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <small>Additional charges apply.</small>	

- **Agregar almacenamiento:** mantiene las opciones de almacenamiento predeterminadas.
- **Agregar etiquetas:** Ingrese etiquetas para la instancia, si lo desea.
- **Configurar grupo de seguridad:** especifique los métodos de conexión necesarios para la instancia del agente de consola: SSH, HTTP y HTTPS.
- **Revisar:** Revise sus selecciones y seleccione **Iniciar**.

Resultado

AWS inicia el software con la configuración especificada. El agente de consola se implementa en aproximadamente cinco minutos.

¿Qué sigue?

Configurar la consola.

Mercado de Azure Gov

Antes de empezar

Debes tener lo siguiente:

- Una red virtual y una subred que cumple con los requisitos de red.

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

- Un rol personalizado de Azure que incluye los permisos necesarios para el agente de consola.

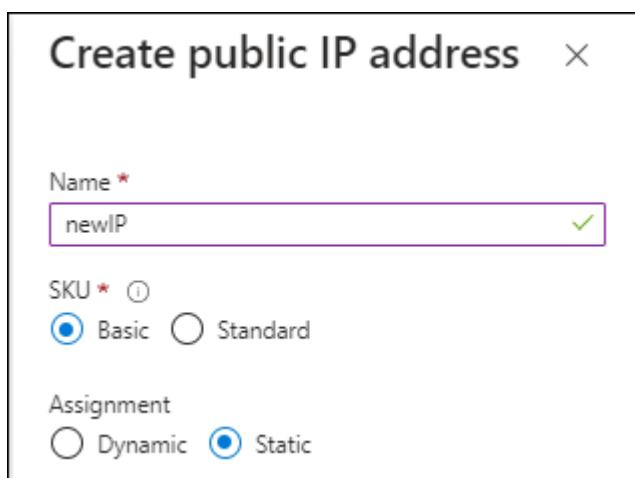
["Aprenda a configurar los permisos de Azure"](#)

Pasos

1. Vaya a la página de la máquina virtual del agente de la NetApp Console en Azure Marketplace.
 - ["Página de Azure Marketplace para regiones comerciales"](#)
 - ["Página de Azure Marketplace para las regiones de Azure Government"](#)
2. Seleccione **Obtenerlo ahora** y luego seleccione **Continuar**.
3. Desde el portal de Azure, seleccione **Crear** y siga los pasos para configurar la máquina virtual.

Tenga en cuenta lo siguiente al configurar la máquina virtual:

- **Tamaño de VM:** elija un tamaño de VM que cumpla con los requisitos de CPU y RAM. Recomendamos Standard_D8s_v3.
- **Discos:** El agente de consola puede funcionar de manera óptima con discos HDD o SSD.
- **IP pública:** para utilizar una dirección IP pública con la máquina virtual del agente de consola, seleccione un SKU básico.



Si utiliza una dirección IP de SKU estándar, la consola utiliza la dirección IP *privada* del agente de la consola, en lugar de la IP pública. Si la máquina que utiliza para acceder a la consola no puede

alcanzar la dirección IP privada, la consola no funciona.

"Documentación de Azure: SKU de IP pública"

- **Grupo de seguridad de red:** el agente de consola requiere conexiones entrantes mediante SSH, HTTP y HTTPS.

"[Ver las reglas del grupo de seguridad para Azure](#)".

- **Identidad:** En **Administración**, seleccione **Habilitar identidad administrada asignada por el sistema**.

Una identidad administrada permite que la máquina virtual del agente de consola se identifique con Microsoft Entra ID sin credenciales. "[Obtenga más información sobre las identidades administradas para los recursos de Azure](#)".

4. En la página **Revisar + crear**, revise sus selecciones y seleccione **Crear** para iniciar la implementación.

Resultado

Azure implementa la máquina virtual con la configuración especificada. La máquina virtual y el software del agente de consola deberían ejecutarse en aproximadamente cinco minutos.

¿Qué sigue?

Configurar la NetApp Console.

Instalación manual (se debe usar para Google Cloud)

Puede instalar el agente de consola manualmente en su propio host Linux que se ejecuta en AWS, Azure o Google Cloud.

Antes de empezar

Debes tener lo siguiente:

- Privilegios de root para instalar el agente de consola.
- Detalles sobre un servidor proxy, si se requiere un proxy para el acceso a Internet desde el agente de la consola.

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

- Un certificado firmado por una CA, si el servidor proxy usa HTTPS o si el proxy es un proxy interceptor.



No es posible configurar un certificado para un servidor proxy transparente al instalar manualmente el agente de consola. Si necesita configurar un certificado para un servidor proxy transparente, debe utilizar la Consola de mantenimiento después de la instalación. Obtén más información sobre "[Consola de mantenimiento del agente](#)".

- Debe deshabilitar la comprobación de configuración que verifica la conectividad saliente durante la instalación. La instalación manual falla si esta comprobación no está deshabilitada. "[Aprenda cómo deshabilitar las comprobaciones de configuración para instalaciones manuales](#)."
- Dependiendo de su sistema operativo, se requiere Podman o Docker Engine antes de instalar el agente de consola.

Acerca de esta tarea

Después de la instalación, el agente de consola se actualiza automáticamente si hay una nueva versión disponible.

Pasos

- Si las variables del sistema `http_proxy` o `https_proxy` están configuradas en el host, elimínelas:

```
unset http_proxy  
unset https_proxy
```

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

- Descargue el software del agente de consola y luego cópielo al host Linux. Puede descargarlo desde la NetApp Console o desde el sitio de soporte de NetApp .

- NetApp Console: vaya a **Agentes > Administración > Implementar agente > Local > Instalación manual**.

Elija descargar los archivos de instalación del agente o una URL a los archivos.

- Sitio de soporte de NetApp (necesario si aún no tiene acceso a la consola) "[Sitio de soporte de NetApp](#)" ,

- Asignar permisos para ejecutar el script.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

Donde <versión> es la versión del agente de consola que descargó.

- Si realiza la instalación en un entorno de nube gubernamental, desactive las comprobaciones de configuración. "[Aprenda cómo deshabilitar las comprobaciones de configuración para instalaciones manuales](#)."
- Ejecute el script de instalación.

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

Tendrás que añadir información del proxy si tu red requiere un proxy para acceder a internet. Puedes añadir un proxy explícito durante la instalación. Los parámetros `--proxy` y `--cacert` son opcionales y no se te pedirá que los añadas. Si tienes un servidor proxy explícito, tendrás que ingresar los parámetros como se muestra.



Si quieres configurar un proxy transparente, puedes hacerlo después de la instalación.
["Obtenga información sobre la consola de mantenimiento del agente."](#)

+

A continuación se muestra un ejemplo de configuración de un servidor proxy explícito con un certificado

firmado por una CA:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

+

--proxy configura el agente de Console para usar un servidor proxy HTTP o HTTPS usando uno de los siguientes formatos:

```
+ * http://address:port * http://user-name:password@address:port * http://domain-name%92user-  
name:password@address:port * https://address:port * https://user-name:password@address:port *  
https://domain-name%92user-name:password@address:port
```

+ Ten en cuenta lo siguiente:

+ **El usuario puede ser un usuario local o un usuario de dominio.** Para un usuario de dominio, debes usar el código ASCII para una \ como se muestra arriba. **El agente de la Console no admite nombres de usuario ni contraseñas que incluyan el carácter @.** Si la contraseña incluye cualquiera de los siguientes caracteres especiales, debes escapar ese carácter especial anteponiéndole una barra invertida: & o !

+ Por ejemplo:

+ http://bxpproxyuser:netapp1!@dirección:3128

1. Si utilizó Podman, necesitará ajustar el puerto aardvark-dns.

- a. SSH a la máquina virtual del agente de consola.
- b. Abra el archivo podman /usr/share/containers/containers.conf y modifique el puerto elegido para el servicio DNS de Aardvark. Por ejemplo, cámbielo a 54.

```
vi /usr/share/containers/containers.conf
```

Por ejemplo:

```
# Port to use for dns forwarding daemon with netavark in rootful  
bridge  
# mode and dns enabled.  
# Using an alternate port might be useful if other DNS services  
should  
# run on the machine.  
#  
dns_bind_port = 54
```

- a. Reinicie la máquina virtual del agente de consola.

Resultado

El agente de consola ahora está instalado. Al final de la instalación, el servicio del agente de consola (occm) se reinicia dos veces si especificó un servidor proxy.

¿Que sigue?

Configurar la NetApp Console.

Paso 2: Configurar la NetApp Console

Cuando accede a la consola por primera vez, se le solicita que elija una organización para el agente de la consola y debe habilitar el modo restringido.

Antes de empezar

La persona que configura el agente de la consola debe iniciar sesión en la consola utilizando un inicio de sesión que no pertenezca a una organización de la consola.

Si su inicio de sesión está asociado con otra organización, deberá registrarse con un nuevo inicio de sesión. De lo contrario, no verá la opción para habilitar el modo restringido en la pantalla de configuración.

Pasos

1. Abra un navegador web desde un host que tenga una conexión a la instancia del agente de consola e ingrese la siguiente URL del agente de consola que instaló.
2. Regístrese o inicie sesión en la NetApp Console.
3. Después de iniciar sesión, configure la consola:
 - a. Introduzca un nombre para el agente de consola.
 - b. Introduzca un nombre para una nueva organización de la consola.
 - c. Seleccione **¿Está ejecutando en un entorno seguro?**
 - d. Seleccione **Habilitar modo restringido en esta cuenta.**

Tenga en cuenta que no puede cambiar esta configuración una vez creada la cuenta. No puedes habilitar el modo restringido más tarde ni puedes deshabilitarlo más tarde.

Si implementó el agente de consola en una región gubernamental, la casilla de verificación ya está habilitada y no se puede cambiar. Esto se debe a que el modo restringido es el único modo compatible en las regiones gubernamentales.

- a. Seleccione **Comencemos.**

Resultado

El agente de consola ahora está instalado y configurado con su organización de consola. Todos los usuarios deben acceder a la consola utilizando la dirección IP de la instancia del agente de la consola.

¿Que sigue?

Proporcione a la consola los permisos que configuró previamente.

Paso 3: Proporcionar permisos al agente de la consola

Si instaló el agente de consola desde Azure Marketplace o manualmente, deberá otorgar los permisos que configuró anteriormente.

Estos pasos no se aplican si implementó el agente de consola desde AWS Marketplace porque eligió el rol de IAM requerido durante la implementación.

["Aprenda a preparar los permisos en la nube"](#) .

Rol de AWS IAM

Adjunte la función IAM que creó previamente a la instancia EC2 donde instaló el agente de consola.

Estos pasos se aplican solo si instaló manualmente el agente de consola en AWS. Para las implementaciones de AWS Marketplace, ya asoció la instancia del agente de consola con un rol de IAM que incluye los permisos necesarios.

Pasos

1. Vaya a la consola de Amazon EC2.
2. Seleccionar **Instancias**.
3. Seleccione la instancia del agente de consola.
4. Seleccione **Acciones > Seguridad > Modificar rol de IAM**.
5. Seleccione el rol de IAM y seleccione **Actualizar rol de IAM**.

Clave de acceso de AWS

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

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Credenciales de la organización**.
3. Seleccione **Agregar credenciales** y siga los pasos del asistente.
 - a. **Ubicación de credenciales**: seleccione *Amazon Web Services > Agente.
 - b. **Definir credenciales**: ingrese una clave de acceso de AWS y una clave secreta.
 - c. **Suscripción al Marketplace**: asocie una suscripción al Marketplace con estas credenciales suscribiéndose ahora o seleccionando una suscripción existente.
 - d. **Revisar**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Rol de Azure

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

Pasos

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

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

["Documentación de Microsoft Azure: Comprender el alcance de Azure RBAC"](#)

2. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de rol**.
3. En la pestaña **Rol**, seleccione el rol **Operador de consola** y seleccione **Siguiente**.



Operador de consola es el nombre predeterminado proporcionado en la política. Si eligió un nombre diferente para el rol, seleccione ese nombre en su lugar.

4. En la pestaña **Miembros**, complete los siguientes pasos:
 - a. Asignar acceso a una **Identidad administrada**.
 - b. Seleccione **Seleccionar miembros**, seleccione la suscripción en la que se creó la máquina virtual del agente de consola, en **Identidad administrada**, elija **Máquina virtual** y, luego, seleccione la máquina virtual del agente de consola.
 - c. Seleccionar **Seleccionar**.
 - d. Seleccionar **Siguiente**.
 - e. Seleccionar **Revisar + asignar**.
 - f. Si desea administrar recursos en suscripciones de Azure adicionales, cambie a esa suscripción y repita estos pasos.

entidad de servicio de Azure

Proporcione a la NetApp Console las credenciales para la entidad de servicio de Azure que configuró previamente.

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Agregar credenciales** y siga los pasos del asistente.
 - a. **Ubicación de credenciales**: seleccione **Microsoft Azure > Agente**.
 - b. **Definir credenciales**: ingrese información sobre la entidad de servicio de Microsoft Entra que otorga los permisos necesarios:
 - ID de la aplicación (cliente)
 - ID de directorio (inquilino)
 - Secreto del cliente
 - c. **Suscripción al Marketplace**: asocie una suscripción al Marketplace con estas credenciales suscribiéndose ahora o seleccionando una suscripción existente.
 - d. **Revisar**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

La NetApp Console ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Cuenta de servicio de Google Cloud

Asocie la cuenta de servicio con la máquina virtual del agente de consola.

Pasos

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

["Documentación de Google Cloud: Cómo cambiar la cuenta de servicio y los ámbitos de acceso de una instancia"](#)
2. Si desea administrar recursos en otros proyectos, otorgue acceso agregando la cuenta de servicio con el rol de agente de consola a ese proyecto. Necesitarás repetir este paso para cada proyecto.

Suscribirse a NetApp Intelligent Services (modo restringido)

Suscríbete a NetApp Intelligent Services desde el marketplace de tu proveedor de nube para pagar los servicios de datos a una tarifa por hora (PAYGO) o mediante un contrato anual. Si compró una licencia de NetApp (BYOL), también deberá suscribirse a la oferta del mercado. Su licencia siempre se cobra primero, pero se le cobrará la tarifa por hora si excede su capacidad autorizada o si el plazo de la licencia vence.

Una suscripción al mercado permite cobrar por los siguientes servicios de datos con modo restringido:

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

La NetApp Data Classification se habilita a través de su suscripción, pero no hay ningún cargo por utilizar la clasificación.

Antes de empezar

Debe haber implementado previamente un agente de consola para poder suscribirse a los servicios de datos. Debe asociar una suscripción de mercado a las credenciales de la nube conectadas a un agente de consola.

AWS

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Credenciales de la organización**.
3. Seleccione el menú de acciones para un conjunto de credenciales asociadas con un agente de consola y luego seleccione **Configurar suscripción**.

Debe seleccionar las credenciales que estén asociadas con un agente de consola. No se puede asociar una suscripción de Marketplace con credenciales asociadas con la NetApp Console.

AWS Instance Profile			
Type: Instance Profile Connector	297337421911 AWS Account ID	IAM Role	Annual_small_1TB_all_services_first_abb Subscription
			4 View Working Environment Configure Subscription Copy Credentials ID
azure_conn_cred			
Type: Azure Keys Connector	97164c15-9f84-420a-83a6-4f668729d206 Application ID	Tenant ID	3 View Subscriptions 0 Working Environments Edit Credentials Delete Credentials

4. Para asociar las credenciales con una suscripción existente, seleccione la suscripción de la lista desplegable y seleccione **Configurar**.

5. Para asociar las credenciales con una nueva suscripción, seleccione **Agregar suscripción > Continuar** y siga los pasos en AWS Marketplace:

- a. Seleccione **Ver opciones de compra**.
- b. Seleccione **Suscribirse**.
- c. Seleccione **Configurar su cuenta**.

Serás redirigido a la NetApp Console.

- d. Desde la página **Asignación de suscripción**:

- Seleccione las organizaciones o cuentas de la consola con las que desea asociar esta suscripción.
- En el campo **Reemplazar suscripción existente**, elija si desea reemplazar automáticamente la suscripción existente de una organización o cuenta con esta nueva suscripción.

La consola reemplaza la suscripción existente para todas las credenciales de la organización o cuenta con esta nueva suscripción. Si un conjunto de credenciales nunca estuvo asociado con una suscripción, entonces esta nueva suscripción no estará asociada con esas credenciales.

Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

Azur

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Credenciales de la organización**.
3. Seleccione el menú de acciones para un conjunto de credenciales asociadas con un agente de consola y luego seleccione **Configurar suscripción**.

Debe seleccionar las credenciales que estén asociadas con un agente de consola. No se puede asociar una suscripción de Marketplace con credenciales asociadas con la NetApp Console.

4. Para asociar las credenciales con una suscripción existente, seleccione la suscripción de la lista desplegable y seleccione **Configurar**.
5. Para asociar las credenciales con una nueva suscripción, seleccione **Agregar suscripción > Continuar** y siga los pasos en Azure Marketplace:

- a. Si se le solicita, inicie sesión en su cuenta de Azure.
- b. Seleccione **Suscribirse**.
- c. Llene el formulario y seleccione **Suscribirse**.
- d. Una vez completado el proceso de suscripción, seleccione **Configurar cuenta ahora**.

Serás redirigido a la NetApp Console.

- e. Desde la página **Asignación de suscripción**:
 - Seleccione las organizaciones o cuentas de la consola con las que desea asociar esta suscripción.
 - En el campo **Reemplazar suscripción existente**, elija si desea reemplazar automáticamente la suscripción existente de una organización o cuenta con esta nueva suscripción.

La consola reemplaza la suscripción existente para todas las credenciales de la organización o cuenta con esta nueva suscripción. Si un conjunto de credenciales nunca estuvo asociado con una suscripción, entonces esta nueva suscripción no estará asociada con esas credenciales.

Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

Google Cloud

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Credenciales de la organización**.
3. Seleccione el menú de acciones para un conjunto de credenciales asociadas con un agente de consola y luego seleccione **Configurar suscripción**.

The screenshot shows the Google Cloud Service Accounts page. At the top, there is a card for a service account named "Google Cloud" (Type: Service Account). Below the card, there are two sections: "Subscriptions" (1 View) and "Working Environments" (0). On the right side, there is a context menu with three options: "Associate Subscription" (with a hand cursor icon), "Copy Credentials ID" (with a copy icon), and "Delete Credentials".

1. Para configurar una suscripción existente con las credenciales seleccionadas, seleccione un proyecto y una suscripción de Google Cloud de la lista desplegable y luego seleccione **Configurar**.

The screenshot shows the Google Cloud Project settings page. It has two dropdown menus: "Google Cloud Project" set to "OCCM-Dev" and "Subscription" set to "GCP subscription for staging". There is also a blue button labeled "+ Add Subscription".

2. Si aún no tiene una suscripción, seleccione **Agregar suscripción > Continuar** y siga los pasos en Google Cloud Marketplace.



Antes de completar los siguientes pasos, asegúrese de tener privilegios de administrador de facturación en su cuenta de Google Cloud, así como un inicio de sesión en la NetApp Console .

- a. Después de ser redirigido a la "["Página de NetApp Intelligent Services en Google Cloud Marketplace"](#)", asegúrese de que el proyecto correcto esté seleccionado en el menú de navegación superior.



NetApp Intelligent Services

[NetApp, Inc.](#)

Get best-in-class data protection and security for your workloads running on NetApp® ONTAP® storage.

[Subscribe](#)

[Overview](#)

[Pricing](#)

[Documentation](#)

[Support](#)

[Related Products](#)

Overview

NetApp offers a comprehensive suite of intelligent services for your ONTAP systems. They proactively protect critical workloads against evolving cyberthreats, detect and respond to ransomware attacks in real time, eliminate backup windows, and orchestrate a quick recovery in minutes when disaster strikes. NetApp intelligent services and Cloud

A
Ty
La
Ca

b. Seleccione **Suscribirse**.

c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.

d. Seleccione **Suscribirse**.

Este paso envía su solicitud de transferencia a NetApp.

e. En el cuadro de diálogo emergente, seleccione **Registrarse con NetApp, Inc.**

Este paso debe completarse para vincular la suscripción de Google Cloud con su organización o cuenta de Console. El proceso de vinculación de una suscripción no estará completo hasta que seas redirigido desde esta página y luego inicies sesión en la Consola.

Your order request has been sent to NetApp, Inc.



Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

[VIEW ORDERS](#)

[REGISTER WITH NETAPP, INC.](#)

f. Complete los pasos en la página **Asignación de suscripción**:



Si alguien de su organización ya tiene una suscripción al mercado desde su cuenta de facturación, será redirigido a "[la página Cloud Volumes ONTAP dentro de la NetApp Console](#)" en cambio. Si esto no es esperado, comuníquese con su equipo de ventas de NetApp . Google solo permite una suscripción por cuenta de facturación de Google.

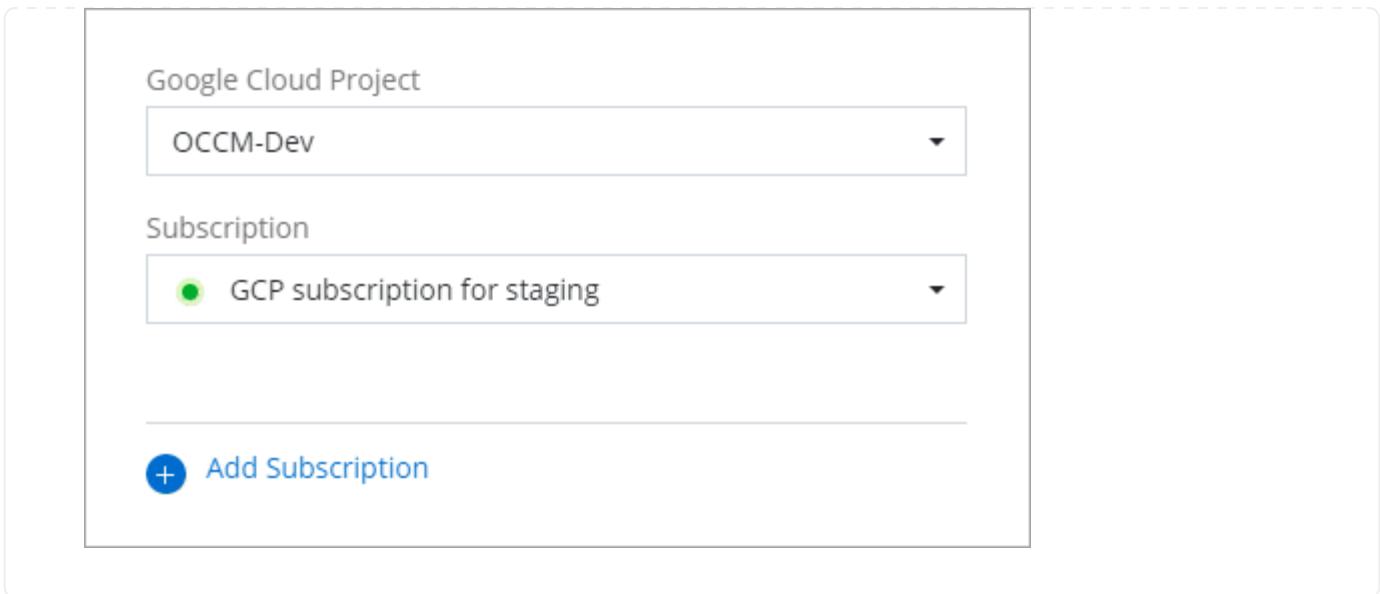
- Seleccione la organización de la consola con la que desea asociar esta suscripción.
- En el campo **Reemplazar suscripción existente**, elija si desea reemplazar automáticamente la suscripción existente de una organización con esta nueva suscripción.

La consola reemplaza la suscripción existente para todas las credenciales de la organización con esta nueva suscripción. Si un conjunto de credenciales nunca estuvo asociado con una suscripción, entonces esta nueva suscripción no estará asociada con esas credenciales.

Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

- Seleccione **Guardar**.

3. Una vez completado este proceso, regrese a la página Credenciales en la Consola y seleccione esta nueva suscripción.



Información relacionada

- "["Administrar licencias BYOL basadas en capacidad para Cloud Volumes ONTAP"](#)"
- "["Administrar licencias BYOL para servicios de datos"](#)"
- "["Administrar credenciales y suscripciones de AWS"](#)"
- "["Administrar credenciales y suscripciones de Azure"](#)"
- "["Administrar credenciales y suscripciones de Google Cloud"](#)"

Qué puedes hacer a continuación (modo restringido)

Una vez que comience a utilizar NetApp Console en modo restringido, podrá comenzar a utilizar los servicios compatibles con el modo restringido.

Para obtener ayuda, consulte la documentación de estos servicios:

- "["Documentación de Azure NetApp Files"](#)"
- "["Documentos de copia de seguridad y recuperación"](#)"
- "["Documentos de clasificación"](#)"
- "["Documentación de Cloud Volumes ONTAP"](#)"
- "["Documentación de la billetera digital"](#)"
- "["Documentación del clúster ONTAP local"](#)"
- "["Documentos de replicación"](#)"

Información relacionada

["Modos de implementación de la NetApp Console"](#)

Información de copyright

Copyright © 2026 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.