Empezar

NetApp Console setup and administration

NetApp
January 27, 2026

Tabla de contenidos

Empezar

Aprenda los conceptos básicos

Obtenga más información sobre la NetApp Console

La consola unifica la gestión y protección del almacenamiento en nubes híbridas múltiples con servicios de datos integrados para proteger y optimizar los datos.

Está disponible como una plataforma de servicio (SaaS) o una opción autohospedada que puede instalar en su nube soberana. Proporciona gestión de almacenamiento, movilidad de datos, protección de datos y análisis y control de datos. Las capacidades de gestión se proporcionan a través de una consola basada en web y API.

Gestión centralizada del almacenamiento

Descubra, implemente y administre el almacenamiento local y en la nube con la consola.

Almacenamiento en la nube y local compatible

Puede administrar los siguientes tipos de almacenamiento desde la consola:

Soluciones de almacenamiento en la nube

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

Almacenamiento de objetos y flash local

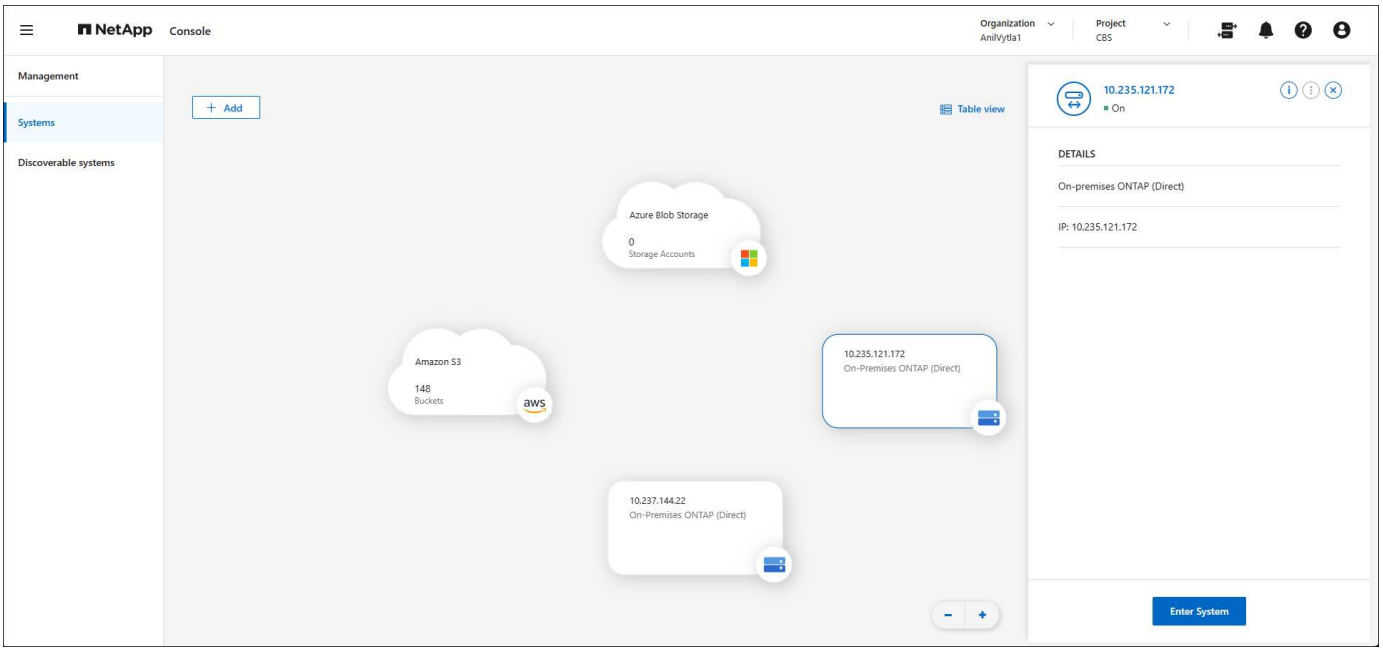
- Sistemas de la serie E
- Clústeres ONTAP
- Sistemas StorageGRID

Almacenamiento de objetos en la nube

- Almacenamiento de Amazon S3
- Almacenamiento de blobs de Azure
- Almacenamiento en la nube de Google

Gestión de almacenamiento

Dentro de la consola, los *sistemas* representan el almacenamiento descubierto o implementado. Puede seleccionar un *sistema* para integrarlo con los servicios de datos de NetApp o administrar el almacenamiento, como agregar volúmenes.



Servicios de datos integrados y gestión de almacenamiento para proteger, asegurar y optimizar los datos

La consola proporciona servicios de datos para proteger y mantener la disponibilidad del almacenamiento.

Alertas de almacenamiento

Vea problemas relacionados con la capacidad, disponibilidad, rendimiento, protección y seguridad en su entorno ONTAP .

Centro de automatización

Utilice soluciones con scripts para automatizar la implementación y la integración de productos y servicios de NetApp .

NetApp Backup and Recovery

Realice copias de seguridad y restaure datos locales y en la nube.

NetApp Data Classification

Prepare la privacidad de los datos de sus aplicaciones y entornos de nube.

NetApp Copy and Sync

Sincronice datos entre almacenes de datos locales y en la nube.

Asesor digital de NetApp (Active IQ)

Utilice análisis predictivos y soporte proactivo para optimizar su infraestructura de datos.

Licenses and subscriptions

Administre y monitoree sus licencias y suscripciones.

NetApp Disaster Recovery

Proteja las cargas de trabajo locales de VMware utilizando VMware Cloud en Amazon FSx para ONTAP como sitio de recuperación ante desastres.

Planificación del ciclo de vida

Identifique clústeres con baja capacidad actual o prevista e implemente niveles de datos o recomendaciones de capacidad adicional.

NetApp Ransomware Resilience

Detecta anomalías que podrían resultar en ataques de ransomware. Proteger y recuperar cargas de trabajo.

NetApp Replication

Replicar datos entre sistemas de almacenamiento para respaldar la copia de seguridad y la recuperación ante desastres.

Actualizaciones de software

Automatice la evaluación, planificación y ejecución de las actualizaciones de ONTAP .

Panel de sostenibilidad

Analice la sostenibilidad de sus sistemas de almacenamiento.

NetApp Cloud Tiering

Amplíe su almacenamiento ONTAP local a la nube.

NetApp Volume Caching

Cree un volumen de caché escribible para acelerar el acceso a los datos o descargar el tráfico de volúmenes con mucho acceso.

Cargas de trabajo de NetApp

Diseñe, configure y opere cargas de trabajo clave utilizando Amazon FSx for NetApp ONTAP.

"Obtenga más información sobre la NetApp Console y los servicios de datos disponibles"

Proveedores de nube compatibles

La consola le permite administrar el almacenamiento en la nube y utilizar servicios en la nube en Amazon Web Services, Microsoft Azure y Google Cloud.

Costo

La NetApp Console es gratuita. Incurrirá en costos si implementa agentes de consola en la nube o utiliza el modo restringido implementado en la nube. Existen costos asociados con algunos servicios de datos de NetApp .https://bluexp.netapp.com/pricing["Obtenga más información sobre los precios de los servicios de datos de NetApp"^]

Cómo funciona la NetApp Console

La NetApp Console es una consola basada en web que se proporciona a través de la capa SaaS, un sistema de gestión de recursos y acceso, agentes de consola que administran sistemas de almacenamiento y habilitan servicios de datos de NetApp , y diferentes modos de implementación para satisfacer los requisitos de su negocio.

Software como servicio

Accedes a la consola a través de un "interfaz basada en web" y API. Esta experiencia SaaS le permite acceder automáticamente a las últimas funciones a medida que se lanzan.

Gestión de identidad y acceso (IAM)

La consola proporciona gestión de identidad y acceso (IAM) para la gestión de recursos y acceso. Este modelo IAM proporciona una gestión granular de recursos y permisos:

- Una *organización* de nivel superior le permite administrar el acceso a sus diversos *proyectos*
- Las *carpetas* le permiten agrupar proyectos relacionados
- La gestión de recursos le permite asociar un recurso con una o más carpetas o proyectos
- La gestión de acceso le permite asignar un rol a los miembros en diferentes niveles de la jerarquía de la organización.
- "Obtenga más información sobre IAM en la NetApp Console"

Agentes de consola

Se necesita un agente de consola para algunas funciones y servicios de datos adicionales. Le permite administrar recursos y procesos en sus entornos locales y en la nube. Lo necesita para administrar algunos sistemas (por ejemplo, Cloud Volumes ONTAP) y para utilizar algunos servicios de datos de NetApp .

"Obtenga más información sobre los agentes de consola" .

Implementación de SaaS versus nube soberana

Puede comenzar a utilizar NetApp Console suscribiéndose a la oferta SaaS o implementándola en su nube soberana. Cuando implementa NetApp Console en una nube soberana, NetApp limita la conectividad saliente para cumplir con los requisitos de seguridad y cumplimiento de su organización. No todas las funciones y servicios están disponibles cuando la consola se implementa en una nube soberana.

NetApp continúa ofreciendo BlueXP para sitios que no desean conectividad saliente. BlueXP se puede instalar en su red sin conectividad saliente. "Obtenga información sobre BlueXP (modo privado) para sitios sin conectividad a Internet."

"Obtenga más información sobre los modos de implementación" .

Certificación SOC 2 Tipo 2

Una firma de contadores públicos certificados independientes y un auditor de servicios examinaron la Consola y afirmaron que logró informes SOC 2 Tipo 2 basados en los criterios de Servicios de Confianza aplicables.

"Ver los informes SOC 2 de NetApp"

Obtenga más información sobre los modos de implementación de la NetApp Console

La NetApp Console ofrece múltiples *modos de implementación* que le permiten satisfacer sus requisitos comerciales y de seguridad.

- El *modo estándar* aprovecha una capa de software como servicio (SaaS) para proporcionar una funcionalidad completa. Los usuarios acceden a la consola a través de una interfaz alojada en la web
- El *modo restringido* está disponible para organizaciones que tienen restricciones de conectividad y desean instalar la NetApp Console en su propia nube pública. Los usuarios acceden a la consola a través de una interfaz basada en web alojada en un agente de consola en su entorno de nube.

NetApp Console restringe el tráfico, la comunicación y los datos en modo restringido, y usted debe asegurarse de que su entorno (local y en la nube) cumpla con las regulaciones requeridas.

Descripción general

Cada modo de implementación difiere en conectividad de salida, ubicación, instalación, autenticación, servicios de datos y métodos de cobro.

Modo estándar

Utiliza un servicio SaaS desde la consola basada en web. Según los servicios de datos y las funciones que planee utilizar, un administrador de la organización de la consola crea uno o más agentes de la consola para administrar los datos dentro de su entorno de nube híbrida.

Este modo utiliza transmisión de datos cifrados a través de Internet público.

Modo restringido

Instala un agente de consola en la nube (en una región gubernamental, soberana o comercial) y tiene conectividad de salida limitada a la capa SaaS de NetApp Console .

Este modo lo suelen utilizar los gobiernos estatales y locales y las empresas reguladas.

Obtenga más información sobre la conectividad saliente a la capa SaaS .

Modo privado de BlueXP (solo interfaz heredada de BlueXP)

El modo privado de BlueXP (interfaz BlueXP heredada) generalmente se usa con entornos locales que no tienen conexión a Internet y con regiones de nube seguras, que incluyen AWS Secret Cloud, AWS Top Secret Cloud y Azure IL6. NetApp continúa brindando soporte a estos entornos con la interfaz BlueXP heredada."Documentación en PDF para el modo privado de BlueXP"

La siguiente tabla proporciona una comparación de la consola de NetApp .

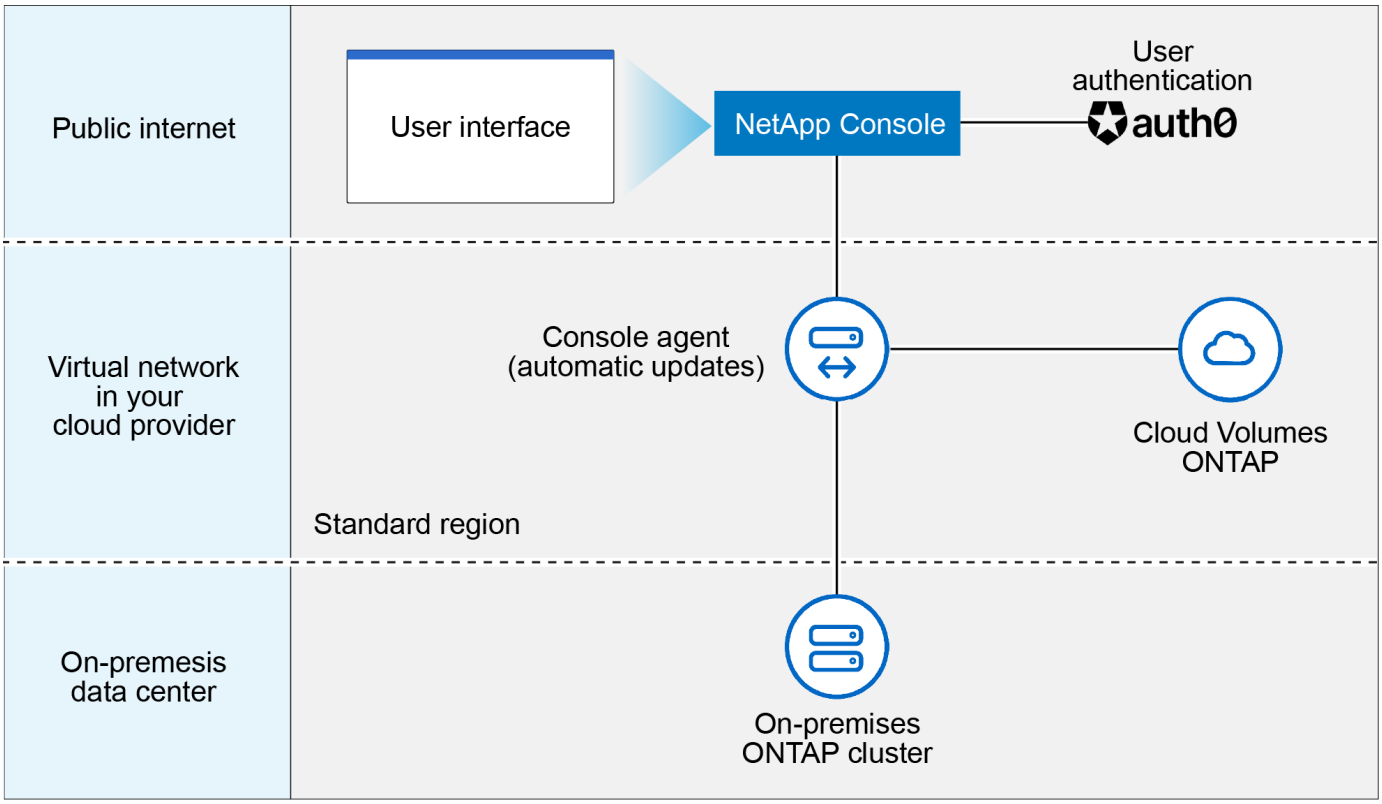
	Modo estándar	Modo restringido
¿Se requiere conexión a la capa SaaS de la NetApp Console ?	Sí	Solo salida
¿Es necesario conectarse a su proveedor de nube?	Sí	Sí, dentro de la región
Instalación del agente de consola	Desde la consola, el mercado en la nube o la instalación manual	Mercado en la nube o instalación manual
Actualizaciones del agente de consola	Actualizaciones automáticas	Actualizaciones automáticas
Acceso UI	Desde la capa SaaS de la consola	Localmente desde una máquina virtual del agente
Punto final de API	La capa SaaS de la consola	Un agente de consola
Autenticación	A través de SaaS utilizando auth0, inicio de sesión NSS o federación de identidad	A través de SaaS utilizando auth0 o federación de identidad

	Modo estándar	Modo restringido
Autenticación multifactor	Disponible para usuarios locales	No disponible
Servicios de almacenamiento y datos	Todos son compatibles	Muchos son apoyados
Opciones de licencia de servicios de datos	Suscripciones al Marketplace y BYOL	Suscripciones al Marketplace y BYOL

Lea las siguientes secciones para obtener más información sobre estos modos, incluidas las funciones y servicios de NetApp Console compatibles.

Modo estándar

La siguiente imagen es un ejemplo de una implementación en modo estándar.



La consola funciona de la siguiente manera en modo estándar:

Comunicación saliente

Se requiere conectividad desde un agente de consola a la capa SaaS de consola, a los recursos disponibles públicamente de su proveedor de nube y a otros componentes esenciales para las operaciones diarias.

- "Puntos finales con los que un agente se pone en contacto en AWS"
- "Puntos de conexión con los que contacta un agente en Azure"
- "Puntos finales con los que un agente se comunica en Google Cloud"

Ubicación compatible con un agente

En el modo estándar, un agente cuenta con soporte en la nube o en sus instalaciones.

Instalación del agente de consola

Puede instalar un agente utilizando uno de los siguientes métodos:

- Desde la consola
- Desde AWS o Azure Marketplace
- Desde el SDK de Google Cloud
- Usar manualmente un instalador en un host Linux en su centro de datos o nube
- Utilice el OVA proporcionado en su entorno VCenter.

Actualizaciones del agente de consola

NetApp actualiza automáticamente su agente mensualmente.

Acceso a la interfaz de usuario

Se puede acceder a la interfaz de usuario desde la consola basada en web que se proporciona a través de la capa SaaS.

Punto final de API

Las llamadas API se realizan al siguiente punto final: https://api.bluexp.netapp.com

Autenticación

Autenticación con inicios de sesión con auth0 o del sitio de soporte de NetApp (NSS). La federación de identidad está disponible.

Servicios de datos compatibles

Se admiten todos los servicios de datos de NetApp . "Obtenga más información sobre los servicios de datos de NetApp" .

Opciones de licencia admitidas

Las suscripciones de Marketplace y BYOL son compatibles con el modo estándar; sin embargo, las opciones de licencia admitidas dependen del servicio de datos de NetApp que esté utilizando. Revise la documentación de cada servicio para obtener más información sobre las opciones de licencia disponibles.

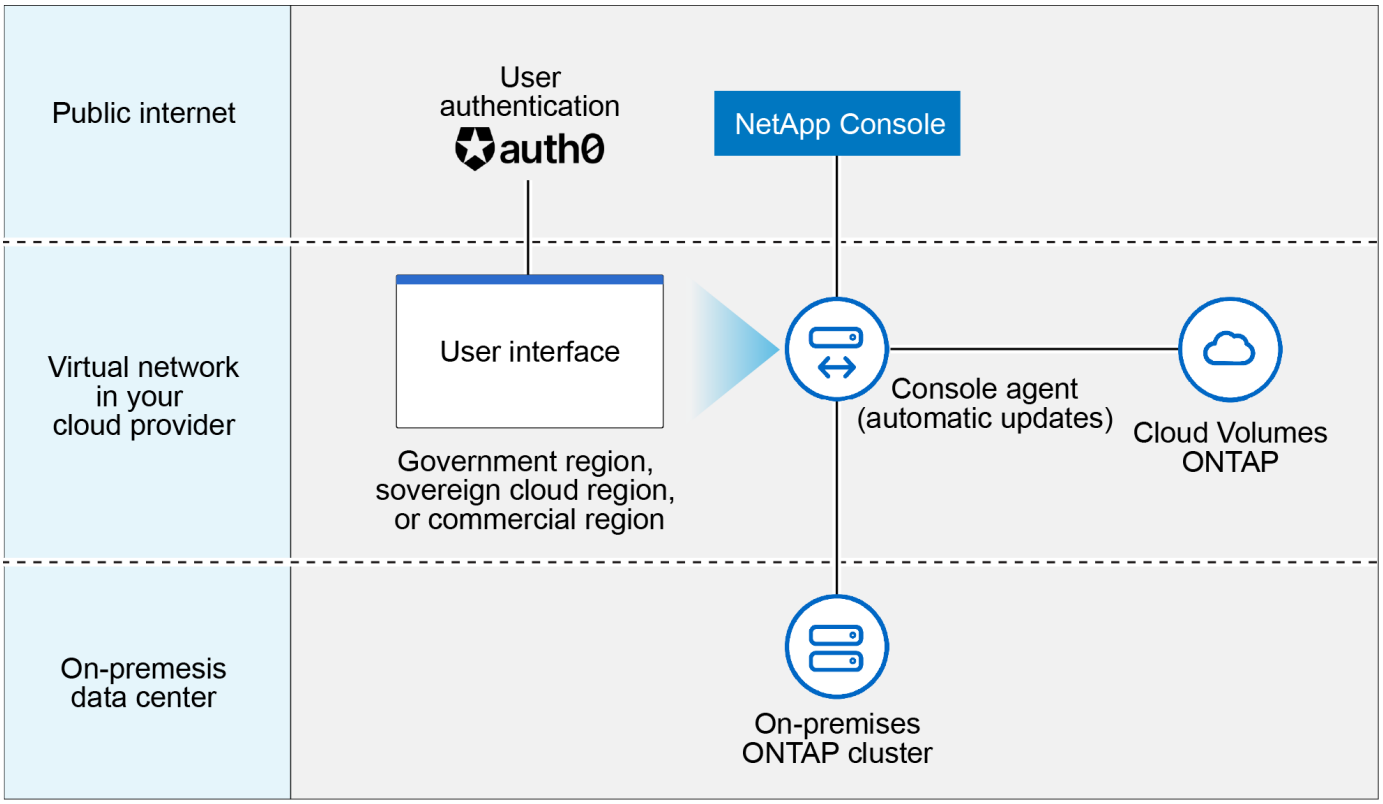
Cómo empezar a utilizar el modo estándar

Ir a la "NetApp Console" y regístrate.

"Aprenda cómo comenzar a utilizar el modo estándar" .

Modo restringido

La siguiente imagen es un ejemplo de una implementación en modo restringido.



La consola funciona de la siguiente manera en modo restringido:

Comunicación saliente

Un agente requiere conectividad saliente a la capa SaaS de la consola para servicios de datos, actualizaciones de software, autenticación y transmisión de metadatos.

La capa SaaS de la consola no inicia la comunicación con un agente. Los agentes inician toda la comunicación con la capa SaaS de la consola, extrayendo o enviando datos según sea necesario.

También se requiere una conexión a los recursos del proveedor de la nube desde dentro de la región.

Ubicación compatible con un agente

En el modo restringido, se admite un agente en la nube: en una región gubernamental, una región soberana o una región comercial.

Instalación del agente de consola

Puede instalarlo desde AWS o Azure Marketplace o realizar una instalación manual en su propio host Linux o utilizar un OVA descargable en su entorno VCenter.

Actualizaciones del agente de consola

NetApp actualiza automáticamente el software de su agente con actualizaciones mensuales.

Acceso a la interfaz de usuario

Se puede acceder a la interfaz de usuario desde una máquina virtual de agente implementada en su región de nube.

Punto final de API

Las llamadas API se realizan a la máquina virtual del agente.

Autenticación

La autenticación se proporciona a través de auth0. La federación de identidad también está disponible.

Servicios de datos y gestión de almacenamiento compatibles

Los siguientes servicios de almacenamiento y datos con modo restringido:

Servicios soportados	Notas
Azure NetApp Files	Soporte completo
Copia de seguridad y recuperación	Compatible con regiones gubernamentales y regiones comerciales con modo restringido. No compatible con regiones soberanas con modo restringido. En el modo restringido, NetApp Backup and Recovery solo admite la copia de seguridad y la restauración de datos de volumen ONTAP . "Ver la lista de destinos de respaldo admitidos para datos de ONTAP" No se admite la realización de copias de seguridad ni la restauración de datos de aplicaciones ni de máquinas virtuales.
NetApp Data Classification	Compatible con regiones gubernamentales con modo restringido. No compatible con regiones comerciales ni con regiones soberanas con modo restringido.
Cloud Volumes ONTAP	Soporte completo
Licenses and subscriptions	Puede acceder a la información de licencia y suscripción con las opciones de licencia compatibles que se enumeran a continuación para el modo restringido.
Clústeres ONTAP locales	Se admiten tanto el descubrimiento con un agente de consola como el descubrimiento sin un agente de consola (descubrimiento directo). Cuando descubre un clúster local sin un agente de consola, la vista avanzada (Administrador del sistema) no es compatible.
Replicación	Compatible con regiones gubernamentales con modo restringido. No compatible con regiones comerciales ni con regiones soberanas con modo restringido.

Opciones de licencia admitidas

Las siguientes opciones de licencia son compatibles con el modo restringido:

- Suscripciones al Marketplace (contratos por hora y anuales)

  Tenga en cuenta lo siguiente:

  - Para Cloud Volumes ONTAP, solo se admiten licencias basadas en capacidad.
  - En Azure, no se admiten contratos anuales con regiones gubernamentales.

- Trae tu propia bebida

  Para Cloud Volumes ONTAP, BYOL admite tanto las licencias basadas en capacidad como las licencias basadas en nodos.

Cómo empezar a utilizar el modo restringido

Debe habilitar el modo restringido al crear su organización de NetApp Console .

Si aún no tiene una organización, se le solicitará que cree su organización y habilite el modo restringido cuando inicie sesión en la Consola por primera vez desde un agente de Consola que instaló manualmente o que creó desde el mercado de su proveedor de nube.

No se puede cambiar la configuración del modo restringido después de crear la organización.

"Aprenda cómo comenzar a utilizar el modo restringido" .

Comparación de servicios y características

La siguiente tabla puede ayudarle a identificar rápidamente qué servicios y funciones son compatibles con el modo restringido.

Tenga en cuenta que algunos servicios podrían ser compatibles con limitaciones. Para obtener más detalles sobre cómo se admiten estos servicios con el modo restringido, consulte las secciones anteriores.

Área de productos	Servicio o característica de datos de NetApp	Modo restringido
Almacenamiento Esta parte de la tabla enumera el soporte para la administración de sistemas de almacenamiento desde la consola. No indica los destinos de respaldo admitidos para NetApp Backup and Recovery.	Amazon FSx para ONTAP	No
	Amazon S3	No
	Blob de Azure	No
	Azure NetApp Files	Sí
	Cloud Volumes ONTAP	Sí
	Google Cloud NetApp Volumes	No
	Almacenamiento en la nube de Google	No
	Clústeres ONTAP locales	Sí
	Serie E	No
	StorageGRID	No

Área de productos	Servicio o característica de datos de NetApp	Modo restringido
Servicios de datos	Copia de seguridad y recuperación de NetApp	Síhttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["Ver la lista de destinos de respaldo admitidos para los datos de volumen de ONTAP"^]
	NetApp Data Classification	Sí
	NetApp Copy and Sync	No
	NetApp Disaster Recovery	No
	NetApp Ransomware Resilience	No
	NetApp Replication	Sí
	NetApp Cloud Tiering	No
	Almacenamiento en caché de volumen de NetApp	No
	Fábrica de cargas de trabajo de NetApp	No
Características	Alertas	No
	Digital Advisor	No
	Gestión de licencias y suscripciones	Sí
	Gestión de identidad y acceso	Sí
	Cartas credenciales	Sí
	Federación	Sí
	Planificación del ciclo de vida	No
	Autenticación multifactor	Sí
	Cuentas NSS	Sí
	Notificaciones	Sí
	Buscar	Sí
	Actualizaciones de software	No
	Sostenibilidad	No
	Auditoría	Sí

Administrar las credenciales NSS asociadas con la NetApp Console

Asocie una cuenta del sitio de soporte de NetApp con su organización de consola para habilitar flujos de trabajo clave para la administración del almacenamiento. Estas credenciales NSS están asociadas con toda la organización.

La consola también admite la asociación de una cuenta NSS por cuenta de usuario. "Aprenda a administrar las credenciales a nivel de usuario" .

Descripción general

Es necesario asociar las credenciales del sitio de soporte de NetApp con el número de serie de su cuenta de consola específica para habilitar las siguientes tareas:

- Implementación de Cloud Volumes ONTAP cuando trae su propia licencia (BYOL)

  Es necesario proporcionar su cuenta NSS para que la consola pueda cargar su clave de licencia y habilitar la suscripción por el período que compró. Esto incluye actualizaciones automáticas para renovaciones de plazos.

- Registro de sistemas Cloud Volumes ONTAP de pago por uso

  Es necesario proporcionar su cuenta NSS para activar el soporte para su sistema y obtener acceso a los recursos de soporte técnico de NetApp .

- Actualización del software Cloud Volumes ONTAP a la última versión

Estas credenciales están asociadas con el número de serie de su cuenta de consola específica. Los usuarios pueden acceder a estas credenciales desde **Soporte > Administración de NSS**.

Agregar una cuenta NSS

Puede agregar y administrar sus cuentas del sitio de soporte de NetApp para usarlas con la consola desde el Panel de soporte dentro de la consola.

Cuando haya agregado su cuenta NSS, la consola utilizará esta información para cosas como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.

Puede asociar varias cuentas NSS a su organización; sin embargo, no puede tener cuentas de clientes y cuentas de socios dentro de la misma organización.

NetApp utiliza Microsoft Entra ID como proveedor de identidad para servicios de autenticación específicos de soporte y licencias.

Pasos

1. En **Administración > Soporte**.
2. Seleccione **Administración NSS**.
3. Seleccione **Agregar cuenta NSS**.
4. Seleccione **Continuar** para ser redirigido a una página de inicio de sesión de Microsoft.
5. En la página de inicio de sesión, proporcione su dirección de correo electrónico y contraseña registradas en el sitio de soporte de NetApp .

   Tras iniciar sesión correctamente, NetApp almacenará el nombre de usuario NSS.

   Esta es una identificación generada por el sistema que se asigna a su correo electrónico. En la página **Administración de NSS**, puede mostrar su correo electrónico desde el ••• menú.

   - Si alguna vez necesita actualizar sus tokens de credenciales de inicio de sesión, también hay una opción **Actualizar credenciales** en el ••• menú.

Al utilizar esta opción se le solicitará que inicie sesión nuevamente. Tenga en cuenta que el token de estas cuentas caduca después de 90 días. Se publicará una notificación para avisarle de esto.

¿Que sigue?

Los usuarios ahora pueden seleccionar la cuenta al crear nuevos sistemas Cloud Volumes ONTAP y al registrar sistemas Cloud Volumes ONTAP existentes.

- "Lanzamiento de Cloud Volumes ONTAP en AWS"
- "Lanzamiento de Cloud Volumes ONTAP en Azure"
- "Lanzamiento de Cloud Volumes ONTAP en Google Cloud"
- "Registro de sistemas de pago por uso"

Actualizar las credenciales de NSS

Por razones de seguridad, debe actualizar sus credenciales NSS cada 90 días. Se le notificará en el centro de notificaciones de la consola si su credencial NSS ha expirado. "Obtenga más información sobre el Centro de notificaciones" .

Las credenciales vencidas pueden afectar lo siguiente, pero no se limitan a:

- Actualizaciones de licencia, lo que significa que no podrá aprovechar la capacidad recién adquirida.
- Capacidad de enviar y realizar seguimiento de casos de soporte.

Además, puede actualizar las credenciales NSS asociadas con su organización si desea cambiar la cuenta NSS asociada con su organización. Por ejemplo, si la persona asociada a su cuenta NSS ha abandonado su empresa.

Pasos

1. En **Administración > Soporte**.
2. Seleccione **Administración NSS**.
3. Para la cuenta NSS que desea actualizar, seleccione ••• y luego seleccione **Actualizar credenciales**.
4. Cuando se le solicite, seleccione **Continuar** para ser redirigido a una página de inicio de sesión de Microsoft.

   NetApp utiliza Microsoft Entra ID como proveedor de identidad para servicios de autenticación relacionados con soporte y licencias.

5. En la página de inicio de sesión, proporcione su dirección de correo electrónico y contraseña registradas en el sitio de soporte de NetApp .

Adjuntar un sistema a una cuenta NSS diferente

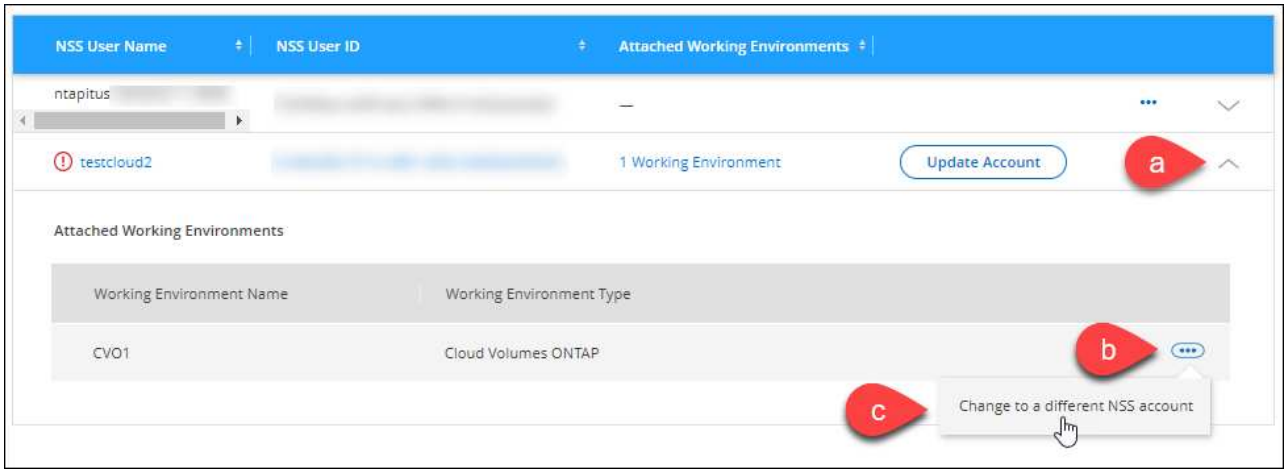
Si su organización tiene varias cuentas de sitio de soporte de NetApp , puede cambiar qué cuenta está asociada con un sistema Cloud Volumes ONTAP .

Primero debes haber asociado la cuenta con la Consola.

Pasos

1. En **Administración > Soporte**.
2. Seleccione **Administración NSS**.

3. Complete los siguientes pasos para cambiar la cuenta NSS:
   a. Expanda la fila de la cuenta del sitio de soporte de NetApp con la que está asociado actualmente el sistema.
   b. Para el sistema cuya asociación desea cambiar, seleccione •••
   c. Seleccione **Cambiar a una cuenta NSS diferente**.



   d. Seleccione la cuenta y luego seleccione **Guardar**.

Mostrar la dirección de correo electrónico de una cuenta NSS

Por seguridad, la dirección de correo electrónico asociada a una cuenta NSS no se muestra de forma predeterminada. Puede ver la dirección de correo electrónico y el nombre de usuario asociado a una cuenta NSS.

Cuando accede a la página de administración de NSS, la consola genera un token para cada cuenta en la tabla. Ese token incluye información sobre la dirección de correo electrónico asociada. El token se elimina cuando abandonas la página. La información nunca se almacena en caché, lo que ayuda a proteger su privacidad.

Pasos

1. En **Administración > Soporte**.
2. Seleccione **Administración NSS**.
3. Para la cuenta NSS que desea actualizar, seleccione ••• y luego seleccione **Mostrar dirección de correo electrónico**. Puede utilizar el botón Copiar para copiar la dirección de correo electrónico.

Eliminar una cuenta NSS

Elimina cualquiera de las cuentas NSS que ya no quieras utilizar con la consola.

No se puede eliminar una cuenta que esté actualmente asociada a un sistema Cloud Volumes ONTAP . Primero necesitasAdjuntar esos sistemas a una cuenta NSS diferente .

Pasos

1. En **Administración > Soporte**.
2. Seleccione **Administración NSS**.

3. Para la cuenta NSS que desea eliminar, seleccione ••• y luego seleccione **Eliminar**.
4. Seleccione **Eliminar** para confirmar.

Obtenga más información sobre los agentes de la NetApp Console

Utilice un agente de consola para conectar NetApp Console a su infraestructura y orquestar de forma segura soluciones de almacenamiento en AWS, Azure, Google Cloud o entornos locales, además de utilizar servicios de protección de datos.

Un agente de consola le permite:

- Organice tareas de administración de almacenamiento desde la NetApp Console, como el aprovisionamiento de Cloud Volumes ONTAP, la configuración de volúmenes de almacenamiento, el uso de la clasificación de datos y más.
- Autenticación mediante los roles IAM de su proveedor de nube para la integración de facturación de suscripciones
- Utilice servicios de datos avanzados (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience y NetApp Cloud Tiering)
- Utilice la consola en modo restringido.

Si no necesita orquestación avanzada ni protección de datos, puede administrar de forma centralizada los clústeres ONTAP locales y los servicios de almacenamiento nativos de la nube sin implementar un agente. También están disponibles herramientas de monitorización y movilidad de datos.

La siguiente tabla muestra qué funciones y servicios puede utilizar con y sin un agente de consola.

	Disponible con agente	**Disponible sin agente**
Sistemas de almacenamiento compatibles:		
Amazon FSx para ONTAP	Sí (funciones de descubrimiento y gestión)	Sí (sólo descubrimiento)
Almacenamiento de Amazon S3	Sí	No
Almacenamiento de blobs de Azure	Sí	Sí
Azure NetApp Files	Sí	Sí
Cloud Volumes ONTAP	Sí	No
Sistemas de la serie E	Sí	No
Google Cloud NetApp Volumes	Sí	Sí
Depósitos de almacenamiento de Google Cloud	Sí	No
Sistemas StorageGRID	Sí	No

	Disponible con agente	Disponible sin agente
Clúster ONTAP local (gestión y descubrimiento avanzados)	Sí (gestión y descubrimiento avanzados)	No (sólo descubrimiento básico)
Servicios de gestión de almacenamiento disponibles:		
Alertas	Sí	No
Centro de automatización	Sí	Sí
Digital Advisor (Active IQ)	Sí	No
Gestión de licencias y suscripciones	Sí	No
Eficiencia económica	Sí	No
Métricas del panel de la página de inicio	Sí[2]	No
Planificación del ciclo de vida	Sí	No[1]
Sostenibilidad	Sí	No
Actualizaciones de software	Sí	Sí
Cargas de trabajo de NetApp	Sí	Sí
Servicios de datos disponibles:		
NetApp Backup and Recovery	Sí	No
Clasificación de datos	Sí	No
NetApp Cloud Tiering	Sí	No
NetApp Copy and Sync	Sí	No
NetApp Disaster Recovery	Sí	No
NetApp Ransomware Resilience	Sí	No
NetApp Volume Caching	Sí	No

[1] Puede ver la planificación del ciclo de vida sin un agente de consola, pero se requiere un agente de consola para iniciar acciones.

[2] Las métricas precisas en la página de inicio requieren agentes de consola configurados y de tamaño

adecuado.

Los agentes de consola deben estar operativos en todo momento

Los agentes de consola son una parte fundamental de la NetApp Console. Es su responsabilidad (la del cliente) asegurarse de que los agentes relevantes estén disponibles, operativos y accesibles en todo momento. La consola puede manejar interrupciones breves del agente, pero debe solucionar las fallas de infraestructura rápidamente.

Esta documentación se rige por el EULA. Utilizar el producto fuera de la documentación puede afectar su funcionalidad y sus derechos de EULA.

Ubicaciones compatibles

Puede instalar agentes en las siguientes ubicaciones:

- Servicios web de Amazon
- Microsoft Azure

  Implemente un agente de consola en Azure en la misma región que los sistemas Cloud Volumes ONTAP que administra. Alternativamente, impleméntelo en el "Par de regiones de Azure" . Esto garantiza que se utilice una conexión de Azure Private Link entre Cloud Volumes ONTAP y sus cuentas de almacenamiento asociadas. "Descubra cómo Cloud Volumes ONTAP utiliza un enlace privado de Azure"

- Google Cloud

  Para utilizar la consola y los servicios de datos con Google Cloud, implemente su agente en Google Cloud.

- En sus instalaciones

Comunicación con proveedores de la nube

El agente utiliza TLS 1.3 para todas las comunicaciones con AWS, Azure y Google Cloud.

Modo restringido

Para utilizar la consola en modo restringido, instale un agente de consola y acceda a la interfaz de la consola que se ejecuta localmente en el agente de consola.

"Obtenga más información sobre los modos de implementación de la NetApp Console" .

Cómo instalar un agente de consola

Puede instalar un agente de consola directamente desde la consola, desde el marketplace de su proveedor de nube o instalando manualmente el software en su propio host Linux o en su entorno VCenter.

- "Obtenga más información sobre los modos de implementación de la NetApp Console"
- "Comience a utilizar la NetApp Console en modo estándar"
- "Comience a usar la NetApp Console en modo restringido"

Permisos del proveedor de la nube

Necesita permisos específicos para crear el agente de consola directamente desde la NetApp Console y otro conjunto de permisos para el agente de consola en sí. Si crea el agente de consola en AWS o Azure directamente desde la consola, entonces la consola crea el agente de consola con los permisos que necesita.

Al utilizar la consola en modo estándar, la forma de proporcionar permisos depende de cómo planea crear el agente de la consola.

Para saber cómo configurar permisos, consulte lo siguiente:

- Modo estándar
  - "Opciones de instalación del agente en AWS"
  - "Opciones de instalación del agente en Azure"
  - "Opciones de instalación del agente en Google Cloud"
  - "Configurar permisos en la nube para implementaciones locales"
- "Configurar permisos para el modo restringido"

Para ver los permisos exactos que el agente de la consola necesita para las operaciones diarias, consulte las siguientes páginas:

- "Descubra cómo el agente de la consola utiliza los permisos de AWS"
- "Descubra cómo el agente de consola usa los permisos de Azure"
- "Descubra cómo el agente de la consola utiliza los permisos de Google Cloud"

Es su responsabilidad actualizar las políticas del agente de la consola a medida que se agreguen nuevos permisos en versiones posteriores. Las notas de la versión enumeran nuevos permisos.

Actualizaciones de agente

NetApp actualiza el software del agente mensualmente para agregar funciones y mejorar la estabilidad. Algunas funciones de la consola, como Cloud Volumes ONTAP y la administración de clústeres ONTAP locales, dependen de la versión y la configuración del agente de la consola.

Cuando instala su agente en la nube, el agente de la consola se actualiza automáticamente si tiene acceso a Internet.

Mantenimiento del sistema operativo y de máquinas virtuales

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

Tenga en cuenta que usted (cliente) no necesita detener ningún servicio en el host de Console gent al aplicar actualizaciones de seguridad menores.

Si usted (cliente) necesita detener y luego iniciar la máquina virtual del agente de consola, debe hacerlo desde la consola de su proveedor de nube o mediante los procedimientos estándar para la administración local.

El agente de consola debe estar operativo en todo momento .

Múltiples sistemas y agentes

Un agente puede administrar múltiples sistemas y soportar servicios de datos en la Consola. Puede utilizar un solo agente para administrar varios sistemas según el tamaño de la implementación y los servicios de datos que utilice.

Para implementaciones a gran escala, trabaje con su representante de NetApp para dimensionar su entorno. Comuníquese con el soporte de NetApp si experimenta problemas.

A continuación se muestran algunos ejemplos de implementaciones de agentes:

- Tienes un entorno multicloud (por ejemplo, AWS y Azure) y prefieres tener un agente en AWS y otro en Azure. Cada uno administra los sistemas Cloud Volumes ONTAP que se ejecutan en esos entornos.
- Un proveedor de servicios puede utilizar una organización de consola para brindar servicios a sus clientes y, al mismo tiempo, utilizar otra organización para brindar recuperación ante desastres a una de sus unidades de negocios. Cada organización necesita su propio agente.

Obtenga más información sobre la gestión de identidad y acceso de la NetApp Console

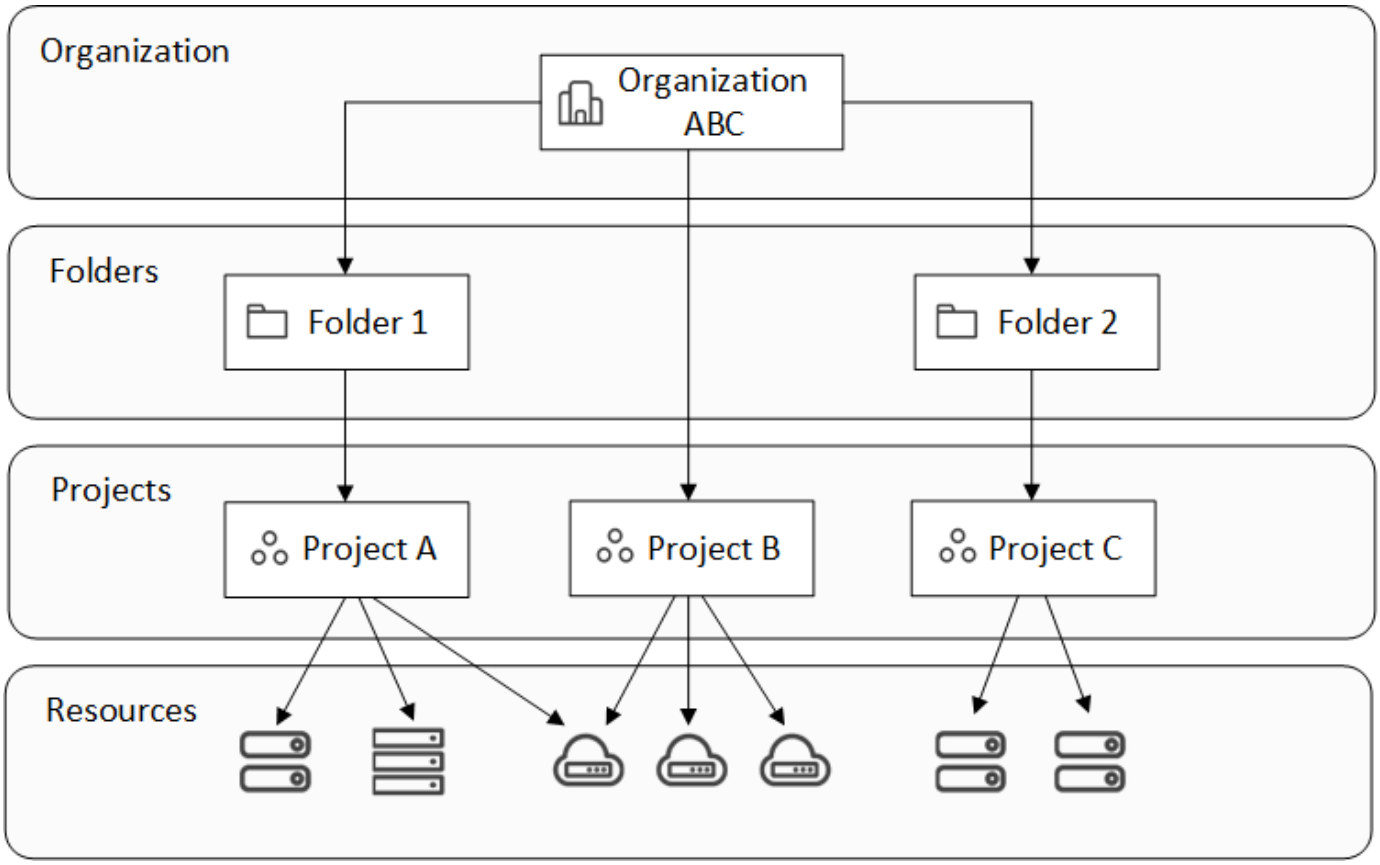
Utilice la gestión de identidad y acceso (IAM) de la consola de NetApp para organizar sus recursos de NetApp y controlar el acceso según la estructura de su negocio: por ubicación, departamento o proyecto.

Los recursos se organizan jerárquicamente: la organización está en la parte superior, seguida de las carpetas (que pueden contener otras carpetas o proyectos) y luego los proyectos, que contienen sistemas de almacenamiento, cargas de trabajo y agentes.

Asigne permisos de control de acceso basado en roles (RBAC) a los miembros a nivel de organización, carpeta o proyecto para garantizar que los usuarios tengan el acceso adecuado a los recursos.

Debe tener los roles de *Superadministrador*, *Administrador de la organización* o *Administrador de carpeta o proyecto* para administrar IAM en NetApp Console.

La siguiente imagen ilustra esta jerarquía en un nivel básico.



]

Componentes de gestión de identidad y acceso

Dentro de NetApp Console, usted organiza sus recursos de almacenamiento utilizando tres componentes principales: componentes organizativos, componentes de recursos y componentes de acceso de usuario.

Proyectos y carpetas dentro de su organización

Dentro de su estructura IAM, usted trabaja con tres componentes organizativos: organizaciones, proyectos y carpetas. Puede conceder acceso a los usuarios asignándoles roles en cualquiera de estos niveles.

Organización

Una *organización* es el nivel superior del sistema IAM de la consola y normalmente representa a su empresa. Su organización consta de carpetas, proyectos, miembros, roles y recursos. Los agentes están asociados con proyectos específicos en la organización.

Proyectos

Un *proyecto* se utiliza para proporcionar acceso a un recurso de almacenamiento. Debes asignar recursos al proyecto antes de que alguien pueda acceder a ellos. Puedes asignar múltiples recursos a un solo proyecto y también puedes tener múltiples proyectos. Luego, asigna permisos a los usuarios del proyecto para darles acceso a los recursos dentro del mismo.

Por ejemplo, puede asociar un sistema ONTAP local con un solo proyecto o con todos los proyectos de su organización, según sus necesidades.

"Aprenda cómo agregar proyectos a su organización."

Carpetas

Agrupe proyectos relacionados en *carpetas* para organizarlos por ubicación, sitio o unidad de negocio. No se pueden asociar recursos directamente con carpetas, pero asignarle a un usuario un rol a nivel de carpeta le da acceso a todos los proyectos en esa carpeta.

"Aprenda cómo agregar carpetas a su organización."

Recursos

Los *recursos* incluyen sistemas de almacenamiento, suscripciones a Keystone y agentes de consola.

+ Debe asociar un recurso a un proyecto antes de que alguien pueda acceder a él.

+

Por ejemplo, puede asociar un sistema Cloud Volumes ONTAP con un proyecto o con todos los proyectos de su organización. La forma de asociar un recurso depende de las necesidades de su organización.

+

"Aprenda a asociar recursos a proyectos."

Sistemas de almacenamiento y suscripciones Keystone

Los sistemas de almacenamiento son los recursos principales que administra en NetApp Console. La NetApp Console admite la gestión de sistemas de almacenamiento locales y en la nube. Debe agregar un sistema de almacenamiento a un proyecto antes de que alguien pueda acceder a él.

Los sistemas de almacenamiento se asocian automáticamente con el proyecto donde se agregan, pero también puedes asociarlos con otros proyectos o carpetas desde la página **Recursos**.

Las suscripciones de Keystone también son recursos que puede asociar con proyectos para otorgar a los usuarios acceso a la suscripción en NetApp Console.

Agentes de consola

Los administradores de la organización crean agentes de consola para administrar los sistemas de almacenamiento y habilitar los servicios de datos de NetApp . Los agentes están inicialmente vinculados al proyecto donde se crean, pero los administradores pueden agregarlos a otros proyectos o carpetas desde la página Agentes.

Asociar un agente a un proyecto permite la gestión de recursos en ese proyecto, mientras que asociar un agente a una carpeta permite a los administradores de carpetas o proyectos decidir qué proyectos deben usar el agente. Los agentes deben estar vinculados a proyectos específicos para proporcionar capacidades de gestión.

"Aprenda a asociar agentes con proyectos."

Miembros y roles

Miembros

Los miembros de su organización son cuentas de usuario o cuentas de servicio. Una cuenta de servicio normalmente es utilizada por una aplicación para completar tareas específicas sin intervención humana.

Debe agregar miembros a su organización después de que se registren en NetApp Console. Una vez agregados, puede asignarles roles para proporcionar acceso a los recursos. Puede agregar manualmente cuentas de servicio desde la consola o automatizar su creación y administración a través de la API IAM de

la NetApp Console .

"Aprenda cómo agregar miembros a su organización."

Roles de acceso

La consola proporciona roles de acceso que puedes asignar a los miembros de tu organización.

Cuando asocias a un miembro con un rol, puedes otorgar ese rol para toda la organización, una carpeta específica o un proyecto específico. El rol que seleccione otorga a un miembro permisos sobre los recursos en la parte seleccionada de la jerarquía.

La NetApp Console proporciona roles granulares que se adhieren a los principios de "mínimo privilegio", lo que significa que los roles de acceso están diseñados para brindar a los usuarios acceso solo a lo que necesitan.

Esto significa que a los usuarios se les pueden asignar múltiples roles a medida que sus funciones se amplían.

"Obtenga más información sobre los roles de acceso" .

Ejemplos de estrategias de IAM

Estrategia de organización pequeña

Para las organizaciones con menos de 50 usuarios y administración de almacenamiento centralizada, considere un enfoque simplificado utilizando roles de superadministrador y supervisor.

Ejemplo: Corporación ABC (equipo de 5 personas)

- **Estructura:** Organización única con 3 proyectos (Producción, Desarrollo, Respaldo)
- **Roles:**
  - 2 miembros senior: rol de **Superadministrador** para acceso administrativo completo
  - 3 miembros del equipo: rol de **Supervisor** para monitoreo sin derechos de modificación
- **Estrategia del agente:** Un solo agente asociado con todos los proyectos para acceso compartido a recursos
- **Beneficios:** Administración simplificada, menor complejidad de roles, adecuado para equipos que requieren un amplio acceso

Estrategia empresarial multirregional

Para organizaciones grandes con operaciones regionales y equipos especializados, implemente un enfoque jerárquico con carpetas que representen límites geográficos o de unidades de negocios.

Ejemplo: Corporación XYZ (empresa multinacional)

- **Estructura:** Organización > Carpetas regionales (Norteamérica, Europa, Asia-Pacífico) > Carpetas de proyectos por región
- **Roles de plataforma:**
  - 1 **Administrador de la organización**: Supervisión global y gestión de políticas
  - 3 **Administradores de carpetas o proyectos**: Control regional (uno por región)
  - 1 **Administrador de la federación**: Integración del proveedor de identidad corporativa

- **Roles de almacenamiento por región:**
  - 9 **Administrador de almacenamiento**: descubre y administra sistemas de almacenamiento en regiones asignadas
  - 2 **Visor de almacenamiento**: Supervise los recursos de almacenamiento en todas las regiones
  - 1 **Especialista en salud del sistema**: Administra la salud del almacenamiento sin modificaciones del sistema
- **Roles de servicio de datos:**
  - **Administrador de copias de seguridad y recuperación**: por proyecto, según las responsabilidades de copia de seguridad
  - **Administrador de resiliencia ante ransomware**: Supervisión del equipo de seguridad en todos los proyectos
- **Estrategia del agente:** Agentes regionales asociados a proyectos geográficos apropiados
- **Beneficios:** Mayor seguridad mediante la segregación de roles, autonomía regional y cumplimiento de las regulaciones locales.

Estrategia de especialización departamental

Para las organizaciones con equipos especializados que requieren acceso a servicios de datos específicos, utilice asignaciones de roles específicas según las responsabilidades funcionales.

Ejemplo: TechCorp (empresa tecnológica de tamaño mediano)

- **Estructura:** Organización > Carpetas departamentales (TI, Seguridad, Desarrollo) > Recursos específicos del proyecto
- **Roles especializados:**
  - Equipo de seguridad: roles de **Administrador de resiliencia contra ransomware** y **Visor de clasificación**
  - Equipo de respaldo: **Superadministrador de respaldo y recuperación** para operaciones de respaldo integrales
  - Equipo de desarrollo: **Administrador de almacenamiento** para la gestión del entorno de prueba
  - Equipo de cumplimiento: **Analista de soporte operativo** para supervisar y respaldar la gestión de casos
- **Estrategia del agente:** Agentes vinculados a proyectos departamentales según la propiedad de los recursos
- **Beneficios:** Control de acceso personalizado, eficiencia operativa mejorada y responsabilidad clara por tareas especializadas

Próximos pasos con IAM en la NetApp Console

- "Comience a usar IAM en la NetApp Console"
- "Supervisar o auditar la actividad de IAM"
- "Obtenga más información sobre la API para NetApp Console IAM"

Comience a usar NetApp Console (Saas)

Flujo de trabajo de introducción (SaaS)

Comience a utilizar la NetApp Console (SaaS) preparando la red para la consola, registrándose y creando una cuenta y utilizando el asistente de la consola para configurar la funcionalidad inicial.

Accede a una consola basada en web que está alojada como un producto de software como servicio (SaaS) de NetApp. Puede utilizar la consola para administrar su entorno de almacenamiento en nube híbrida y utilizar los servicios de datos de NetApp .

"Preparar la red para usar la consola de NetApp"

Asegúrese de que las computadoras que acceden a la consola de NetApp tengan acceso de red a los puntos finales requeridos.

"Aprenda a preparar la red para la consola de NetApp ."

"Regístrate y crea una organización"

Ir a la "Consola de NetApp" y regístrate. Si se le solicita crear una organización y cree que ya existe una para su empresa, cierre el cuadro de diálogo e infórmeselo al administrador de su organización. Si actualmente no hay un administrador de la organización para su empresa, puede reclamar este rol. "Aprenda cómo comunicarse con un administrador de la organización."

En este punto, habrá iniciado sesión y podrá usar el asistente de NetApp para comenzar a configurar la consola. Para comenzar, asocie su cuenta de soporte de NetApp y un agente de consola para habilitar la funcionalidad completa.

Si elige no utilizar el asistente de NetApp o instalar un agente de consola, puede comenzar a administrar el almacenamiento y utilizar servicios como Digital Advisor, Amazon FSx para ONTAP, Azure NetApp Files y más. "Descubra lo que puede hacer sin un agente de consola".

Asocie su cuenta del sitio de soporte de NetApp (NSS)

Asociar su cuenta del sitio de soporte de NetApp (NSS) con la consola le permite administrar sus licencias y suscripciones más fácilmente, así como acceder a recursos de soporte directamente desde la consola.

Crear un agente de consola

Las funciones de administración de almacenamiento avanzada y algunos servicios de datos de NetApp requieren que instale un agente de consola. El agente de la consola permite que la consola administre recursos y procesos dentro de su entorno de nube híbrida.

Puede crear un agente de consola en su nube o red local.

- "Obtenga más información sobre cuándo se requieren los agentes de consola y cómo funcionan"
- "Aprenda a crear un agente de consola en AWS"
- "Aprenda a crear un agente de consola en Azure"
- "Aprenda a crear un agente de consola en Google Cloud"

- "Aprenda a crear un agente de consola local"

5 **Agregar un sistema de almacenamiento a la consola**

Dentro de la NetApp Console, puede agregar o descubrir sistemas de almacenamiento para administrar su entorno de almacenamiento en nube híbrida. Utilice el asistente de NetApp para agregar su primer sistema de almacenamiento.

Si instala un agente de consola en AWS, Microsoft Azure o Google Cloud, la consola descubre automáticamente información sobre los buckets de Amazon S3, Azure Blob Storage o Google Cloud Storage en la ubicación donde está instalado el agente. Estos sistemas se agregan automáticamente a la página **Sistemas**.

- "Aprenda a descubrir un sistema ONTAP"
- "Aprenda a descubrir un sistema StorageGRID"
- "Aprenda a descubrir un sistema de la Serie E"

6 **"Suscríbete a los NetApp Intelligent Services (opcional)"**

Regístrese en NetApp Intelligent Services a través de su proveedor de nube para facturación por hora (PAYGO) o anual. Una suscripción incluye NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience, NetApp Disaster Recovery y NetApp Data Classification.

Preparar el acceso a la red para la NetApp Console

La NetApp Console, el agente de la NetApp Console y los servicios de datos de NetApp requieren acceso a Internet saliente y la capacidad de comunicarse con los puntos finales necesarios.

Necesitará configurar el acceso a la red para lo siguiente:

- Computadoras que acceden a la NetApp Console como software como servicio (SaaS)
- Agentes de consola que se instalan localmente o en la nube. Agentes de consola.

Con 4.0.0, NetApp ha reducido los puntos finales de red necesarios para la consola y los agentes de consola, lo que mejora la seguridad y simplifica la implementación. Es importante destacar que todas las implementaciones anteriores a la versión 4.0.0 continúan siendo totalmente compatibles. Si bien los puntos finales anteriores siguen estando disponibles para los agentes existentes, NetApp recomienda encarecidamente actualizar las reglas de firewall para los puntos finales actuales después de confirmar que las actualizaciones de los agentes fueron exitosas."Aprenda cómo actualizar su lista de puntos finales."

Puntos finales contactados por la NetApp Console y los agentes de la consola

Cada agente que implemente y cada computadora que acceda a la NetApp Console deben tener conexiones a los puntos finales que se enumeran a continuación.

Los agentes de consola que están implementados en su proveedor de nube necesitan acceso a los puntos finales correspondientes a ese proveedor de nube.

Puntos finales	Objetivo
\ 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.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obtener imágenes para las actualizaciones del agente de consola. • 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. 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" . • Cuando actualice los puntos finales actuales en su firewall, sus agentes existentes continuarán funcionando.

Los puntos finales del proveedor de la nube se comunicaron con el agente de la consola

Los agentes de consola deben tener acceso a puntos finales adicionales si están implementados en su proveedor de nube.

Configure el acceso al punto final de la red del proveedor de nube antes de instalar el agente de la consola.

- "Configurar el acceso a la red de AWS para un agente de consola"
- "Configurar el acceso a la red de Azure para un agente de consola"
- "Configurar el acceso a la red de Google Cloud para un agente de la consola"

Puntos finales de servicios de datos contactados por el agente de la consola

Algunos servicios de datos de NetApp , así como Cloud Volumes ONTAP, requieren que el agente tenga

acceso a Internet saliente adicional.

Puntos finales para Cloud Volumes ONTAP

- "Puntos finales para Cloud Volumes ONTAP en AWS"
- "Puntos de conexión para Cloud Volumes ONTAP en Azure"
- "Puntos finales para Cloud Volumes ONTAP en Google Cloud"

Puntos finales para cargas de trabajo

El agente de la consola debe poder acceder al siguiente punto final para las cargas de trabajo de NetApp .

Puntos finales	Objetivo
\ https://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 cargas de trabajo basadas en FSx para ONTAP.

Regístrese o inicie sesión en la NetApp Console

Para utilizar la consola, regístrese o inicie sesión con sus credenciales del sitio de soporte de NetApp , o cree un inicio de sesión para la NetApp Console . Si eres el primero de tu empresa en registrarte, crearás una nueva organización como administrador. Si su empresa ya tiene una organización, regístrese o inicie sesión con sus credenciales existentes del sitio de soporte de NetApp o con el inicio de sesión único (SSO) de la empresa.

Regístrese en NetApp Console como administrador inicial de la organización

Si su empresa no tiene una organización de NetApp Console , regístrese para crear una. El primer usuario se convierte en el administrador de la organización y administra las cuentas de usuario y los permisos. Puede actualizar roles y agregar más administradores más tarde.

Pasos

1. Abra un navegador web y vaya a "NetApp Console"
2. Si tiene una cuenta del sitio de soporte de NetApp , ingrese la dirección de correo electrónico asociada a su cuenta directamente en la página **Iniciar sesión**.

   La consola lo registra como parte de este inicio de sesión inicial con sus credenciales del sitio de soporte de NetApp .

3. Si desea registrarse creando un inicio de sesión de consola, seleccione **Registrarse**.
   a. En la página **Registrarse**, ingrese la información requerida y seleccione **Siguiente**.

      Sólo se permiten caracteres ingleses en el formulario de registro.

   b. Revise su bandeja de entrada en busca de un correo electrónico de NetApp que incluye instrucciones para verificar su dirección de correo electrónico.

Verifique su dirección de correo electrónico para completar el registro.

4. Después de iniciar sesión, revise y acepte el Acuerdo de licencia de usuario final.
5. En la página **Bienvenido**, crea una organización.
6. Seleccione **Comencemos**.

+ Como usuario nuevo y administrador de la organización, seguirá un proceso guiado para agregar recursos de almacenamiento, crear un agente de consola y más. "Obtenga información sobre cómo utilizar el Asistente de consola."

Próximos pasos

Como administrador, después de completar los pasos incluidos en el Asistente de consola, debe planificar su estrategia de identidad y acceso, agregar usuarios a su organización y asignar roles. "Obtenga información sobre la gestión de identidad y acceso para la NetApp Console"

Regístrese o inicie sesión en la NetApp Console cuando ya exista una organización

Si su empresa ya tiene una organización de NetApp Console , regístrese o inicie sesión para acceder a ella. Su método de registro o inicio de sesión depende de si su empresa utiliza la federación de identidad o tiene credenciales del sitio de soporte de NetApp . De lo contrario, cree un inicio de sesión en la NetApp Console .

Pasos

1. Abra un navegador web y vaya a "NetApp Console"
2. Si tiene una cuenta del sitio de soporte de NetApp o si su empresa ha configurado el inicio de sesión único (SSO), ingrese su dirección de correo electrónico asociada o sus credenciales de SSO en la página **Iniciar sesión**. Siga las instrucciones para completar el inicio de sesión.

   En ambos casos, usted se registra en la Consola como parte de este inicio de sesión inicial.

3. Si desea registrarse creando un inicio de sesión de consola, seleccione **Registrarse**.
   a. En la página **Registrarse**, ingrese la información requerida y seleccione **Siguiente**.

      Sólo se permiten caracteres ingleses en el formulario de registro.

   b. Revise su bandeja de entrada en busca de un correo electrónico de NetApp que incluye instrucciones para verificar su dirección de correo electrónico.

      Verifique su dirección de correo electrónico para completar el registro.

4. Después de iniciar sesión, revise y acepte el Acuerdo de licencia de usuario final.
5. Si el sistema le solicita que cree una organización, cierre el cuadro de diálogo e infórmeselo a un administrador de la consola para que pueda agregarlo a su organización de la consola y brindarle acceso. "Aprenda cómo comunicarse con un administrador de la organización."

Próximos pasos

Una vez que tenga acceso a su organización, podrá comenzar a administrar el almacenamiento y utilizar los servicios de datos que se le hayan asignado.

Comience a utilizar el asistente de la NetApp Console

Si es la primera vez que utiliza la NetApp Console (SaaS) con el rol de administrador de

la organización, puede usar el asistente de la consola para que lo guíe a través del proceso de configuración inicial. El asistente le ayuda a agregar una cuenta de NetApp Support Site (NSS), agregar un agente de consola, agregar un clúster y agregar una licencia o suscripción, lo que facilita el inicio de la administración de sus datos.

Roles necesarios para acceder al asistente de la consola

El asistente de consola solo está disponible para usuarios con el rol de administrador de la organización.

De forma predeterminada, la NetApp Console muestra el asistente de la consola en la página de inicio para los usuarios nuevos que tienen el rol de administrador de la organización. Permanecerá disponible hasta que complete las tareas obligatorias de crear un agente de consola y agregar un sistema.

Utilice el asistente para completar estas tareas, que proporcionan la configuración mínima para su entorno de NetApp Console :

- Agregue una cuenta del sitio de soporte de NetApp (NSS).

  "Aprenda cómo agregar una cuenta NSS".

- Conéctese a su patrimonio de almacenamiento implementando un agente de consola.

  "Aprenda a instalar un agente de consola local."

- Administrar un sistema de almacenamiento agregando o descubriendo un clúster
- Agregue una suscripción de mercado o una licencia PAYGO.

  "Aprenda a agregar licencias y suscripciones".

- Revisar la información de los servicios de datos.

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.

"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.

"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		9,6 • 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	Podman versión 5.4.0 con podman-compose 1.5.0. Ver los requisitos de configuración de Podman .
Compatible con modo de aplicación o modo permisivo		9.1 a 9.4 • 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	Podman versión 4.9.4 con podman-compose 1.5.0. Ver los requisitos de configuración de Podman .

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Compatible con modo de aplicación o modo permisivo		8.6 a 8.10 • 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	Podman versión 4.6.1 o 4.9.4 con podman-compose 1.0.6. Ver los requisitos de configuración de Podman .
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.

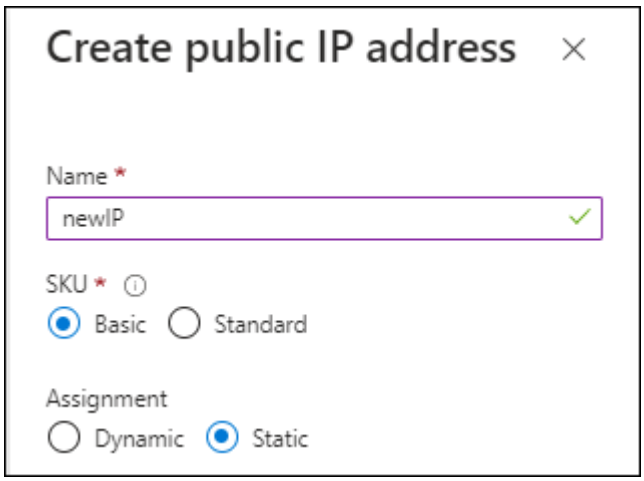
Puntos finales	Objetivo
Entornos AWS	Servicios de AWS (amazonaws.com): • Formación de nubes • Nube de cómputo elástica (EC2) • Gestión de identidad y acceso (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Servicio de almacenamiento simple (S3)
Para administrar los recursos de AWS. El punto final depende de su región de AWS. "Consulte la documentación de AWS para obtener más detalles."	Amazon FsX para NetApp ONTAP: • 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	Para obtener imágenes para las actualizaciones del agente de consola. • 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. 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" . • 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.



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.

"Documentación de Azure: SKU de IP pública"

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 asignable.

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

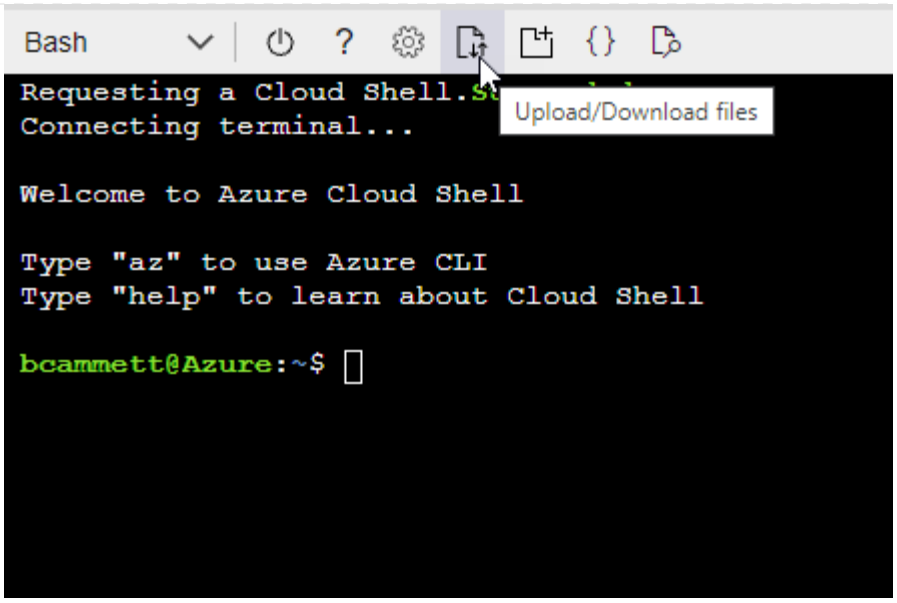
   Ejemplo

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

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

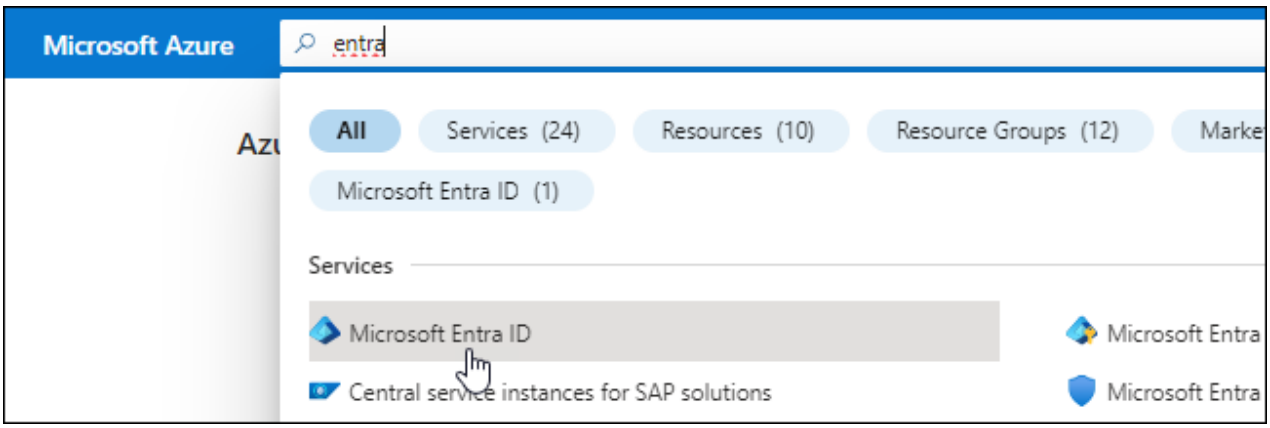
Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita la consola. Debe proporcionar a la consola estas credenciales después de instalar el agente de la consola.

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**.



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 asignable.

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

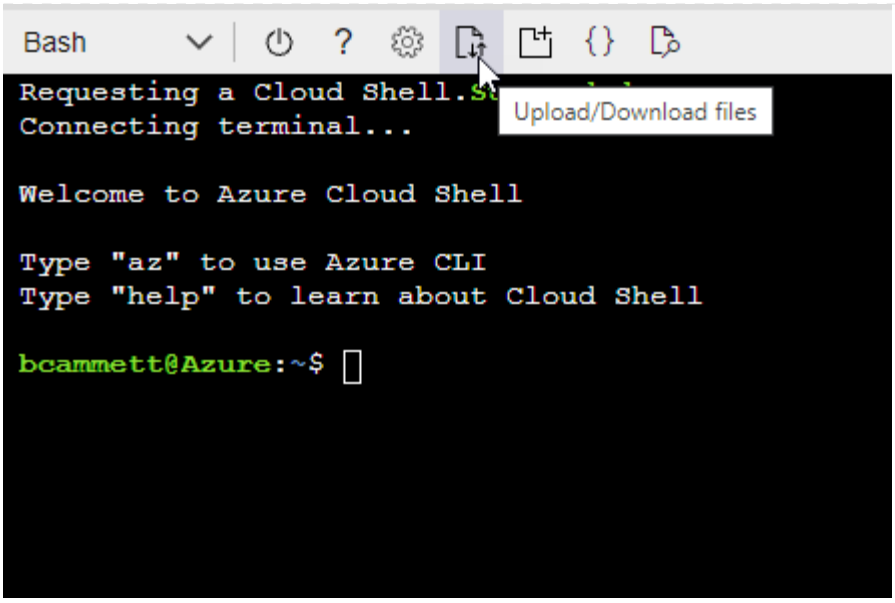
      Ejemplo

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

   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:

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

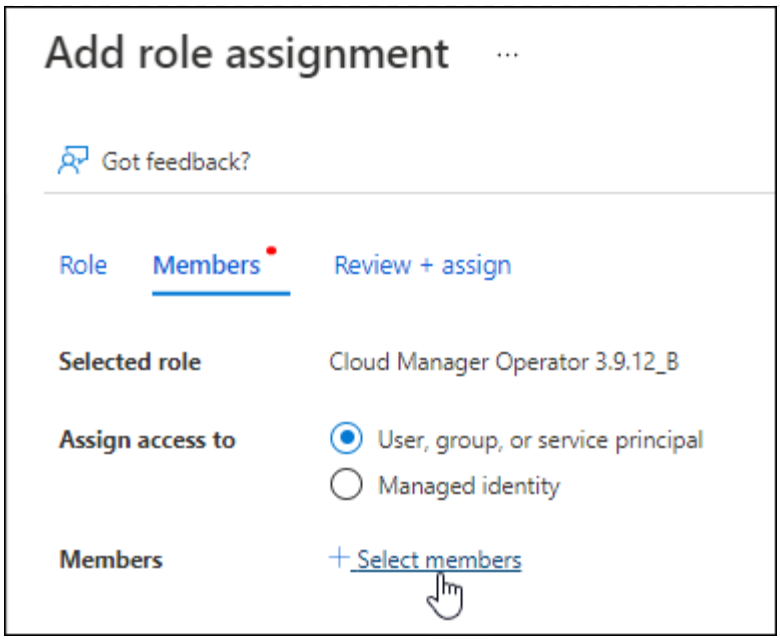
   b. Seleccione la suscripción.

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

   d. En la pestaña **Rol**, seleccione el rol **Operador de consola** y seleccione **Siguiente**.

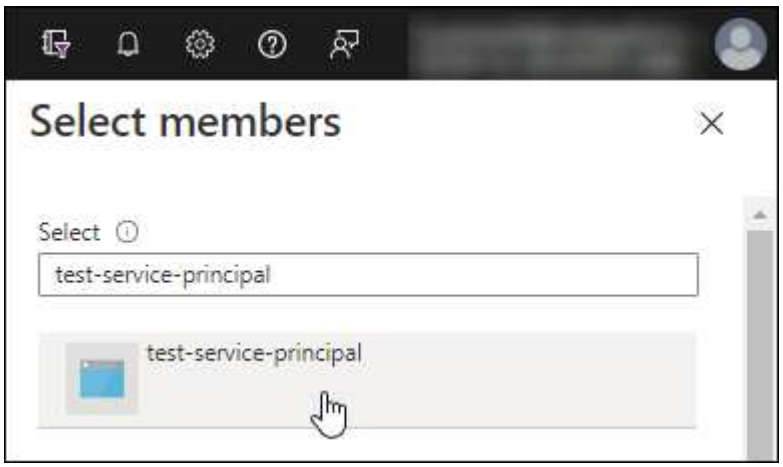
   e. En la pestaña **Miembros**, complete los siguientes pasos:

      - Mantenga seleccionado **Usuario, grupo o entidad de servicio**.
      - Seleccionar **Seleccionar miembros**.



- Busque el nombre de la aplicación.

  He aquí un ejemplo:



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

f. Seleccione **Revisar + asignar**.

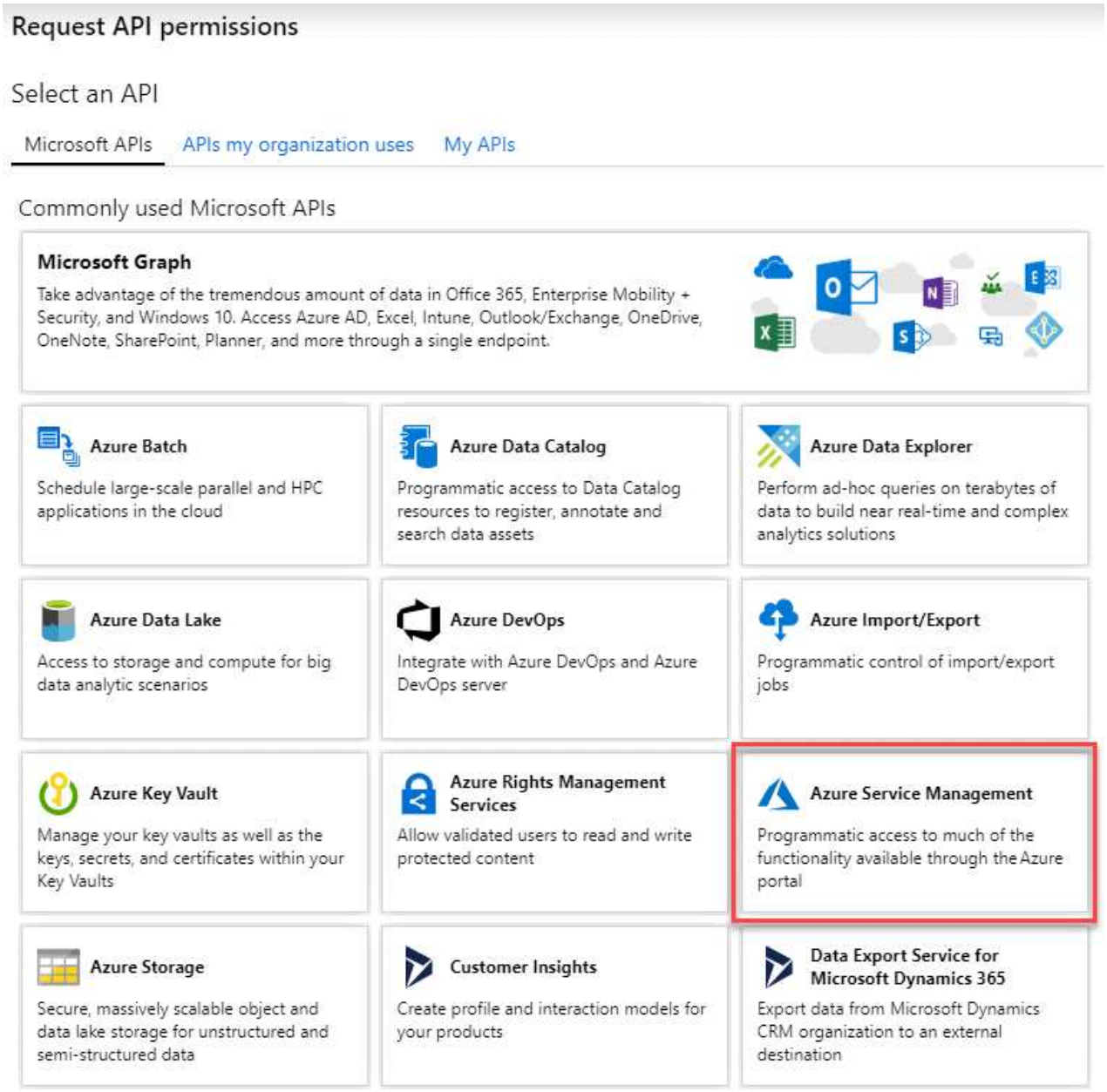
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

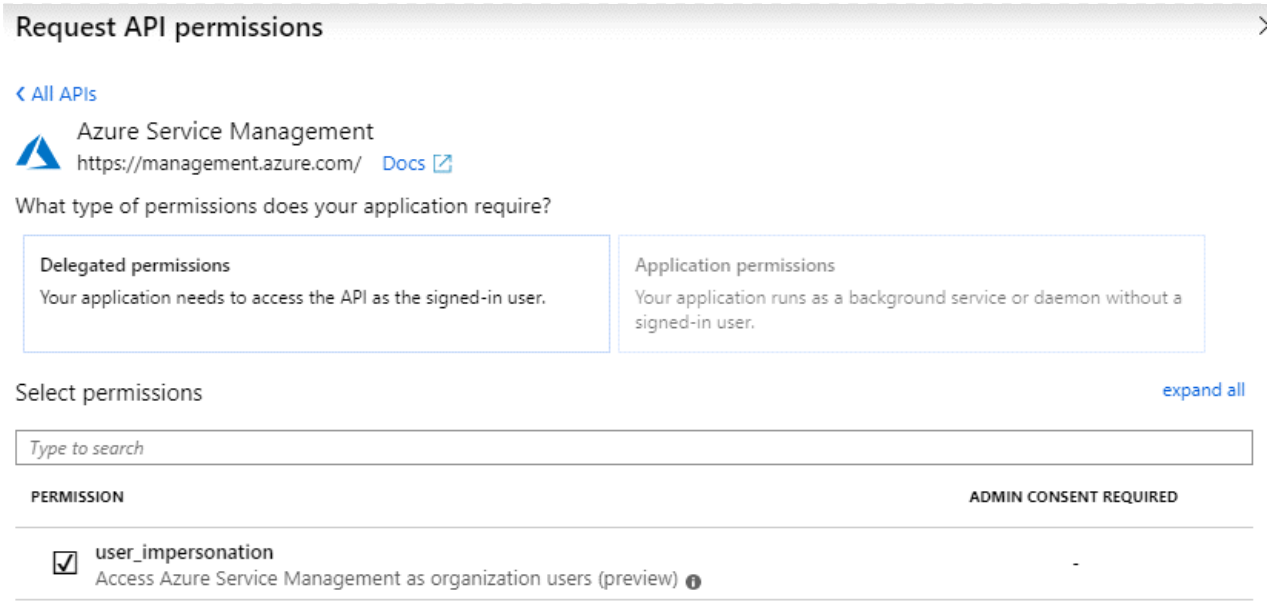
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

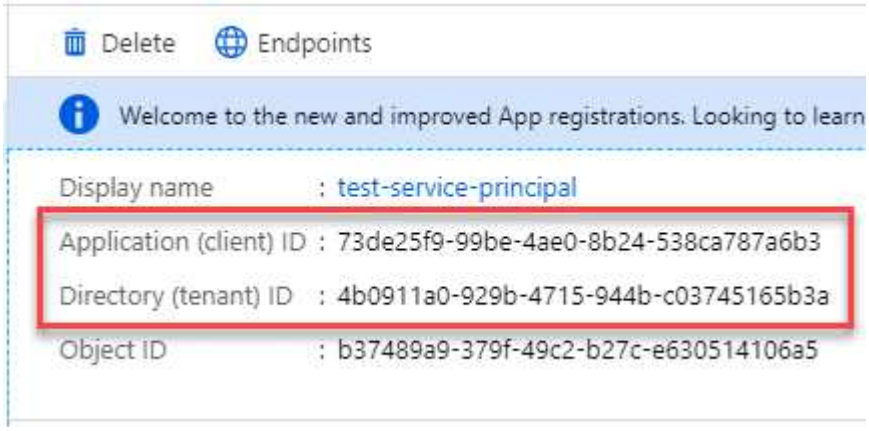


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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)**.



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. Seleccione **Certificados y secretos > Nuevo secreto de cliente**.
4. Proporcione una descripción del secreto y una duración.
5. Seleccione **Agregar**.
6. Copia el valor del secreto del cliente.

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 Infrastructure Manager
    - API de Cloud Deployment Manager V2
    - 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 administración de claves en la nube (KMS)

      (Obligatorio solo si planea utilizar NetApp Backup and Recovery con claves de cifrado administradas por el cliente (CMEK))

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"

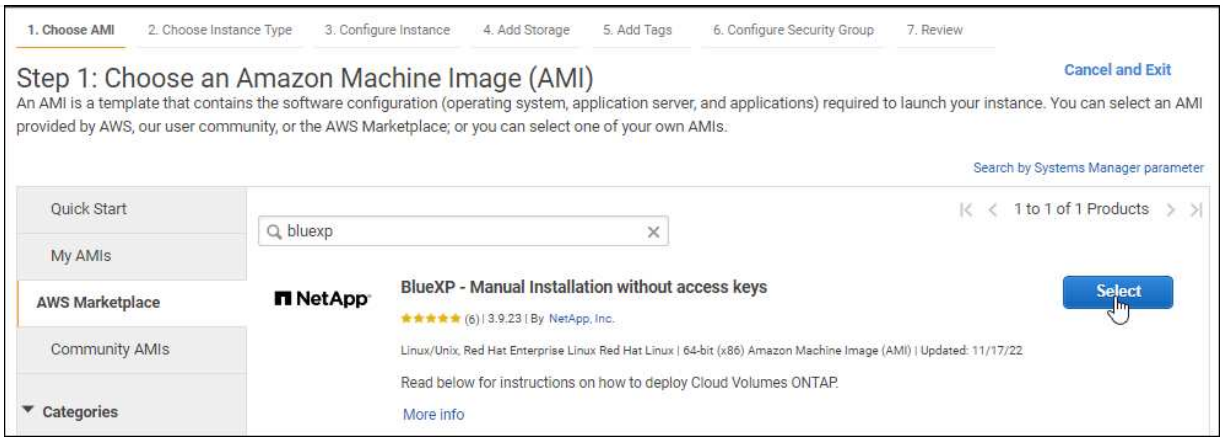
- Una función de IAM con una política adjunta que incluye los permisos necesarios para el agente de la consola.

  "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.



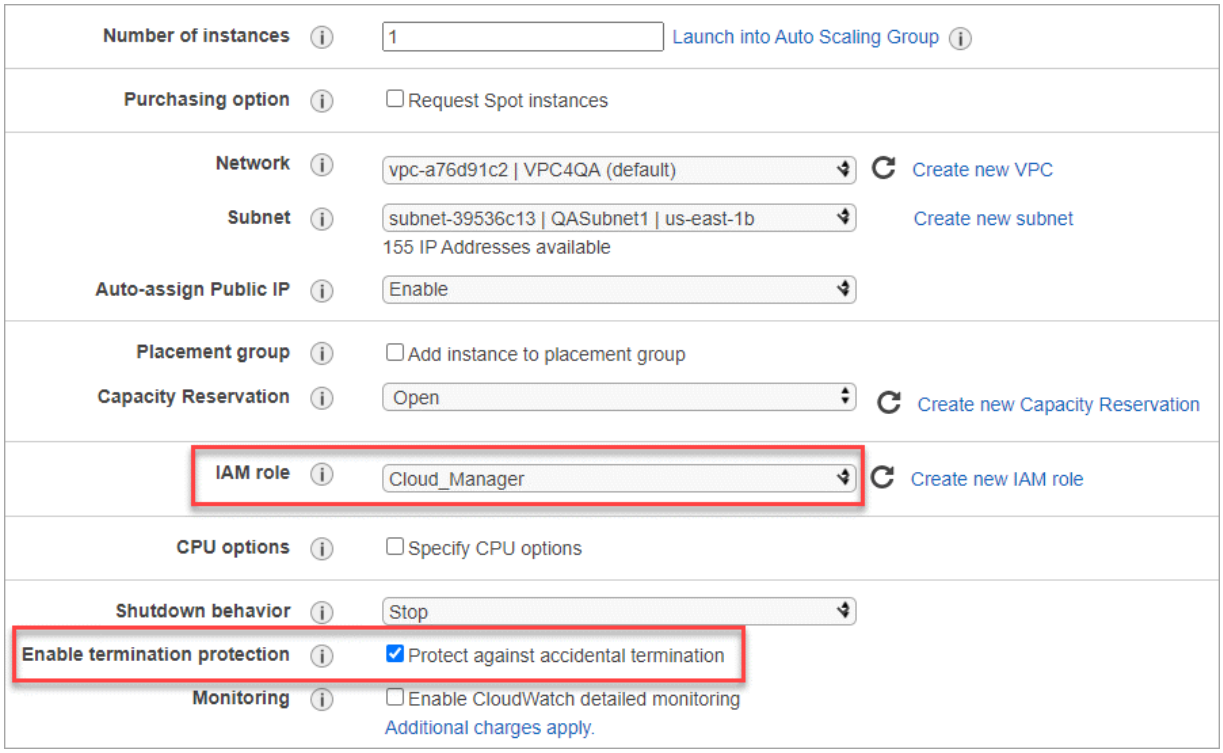
d. Seleccione **Continuar**.

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.



   - **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.

¿Que 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.

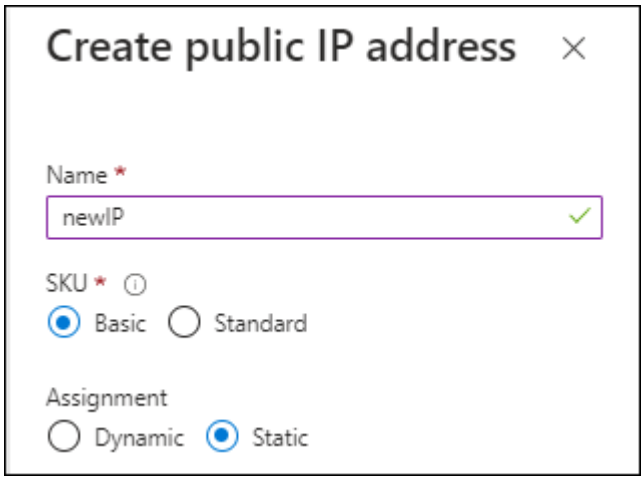
  "Aprenda a configurar los permisos de Azure"

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.

¿Que 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

1. 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.

2. 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" ,
3. Asignar permisos para ejecutar el script.

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

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

4. 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."
5. 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. Seleccione **Siguiente**.
    e. Seleccione **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

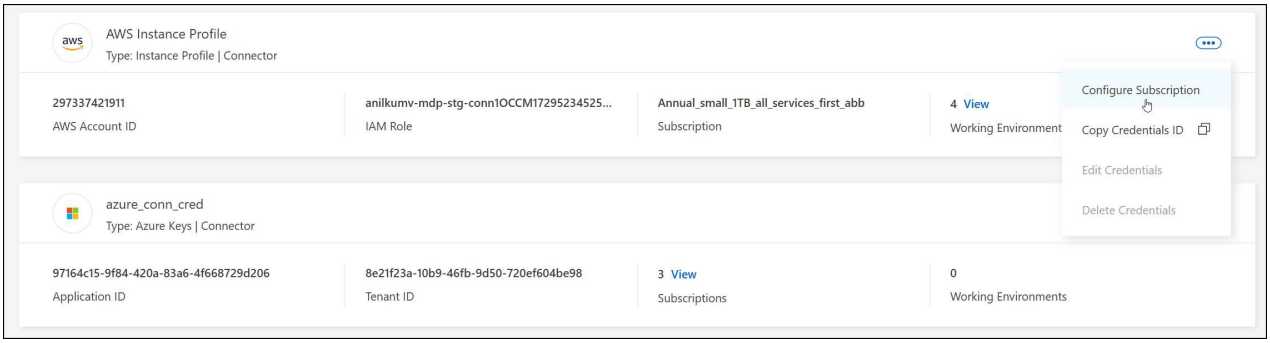
Debe haber implementado previamente un agente de consola para poder suscribirse a los servicios de datos. Debe asociar una suscripción de mercado a las credenciales de la nube conectadas a un agente de consola.

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.



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.

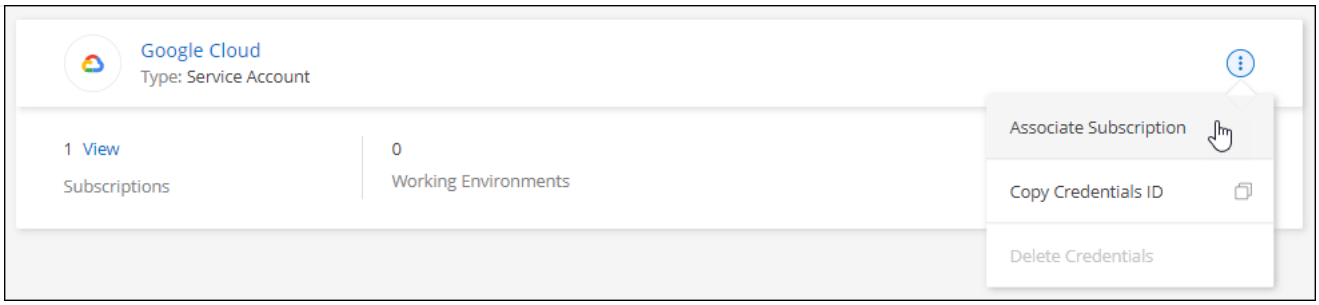
   Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

      - Seleccione **Guardar**.

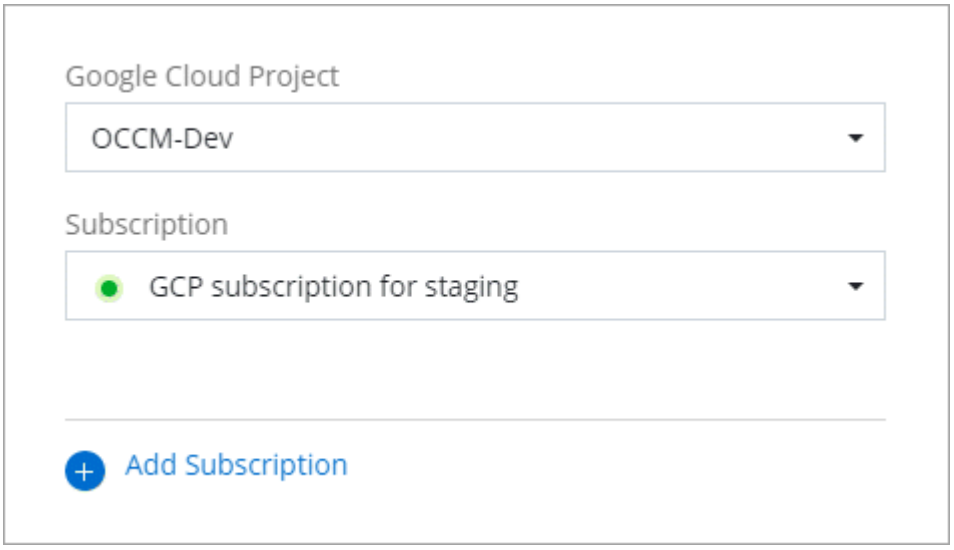
Google Cloud

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**.



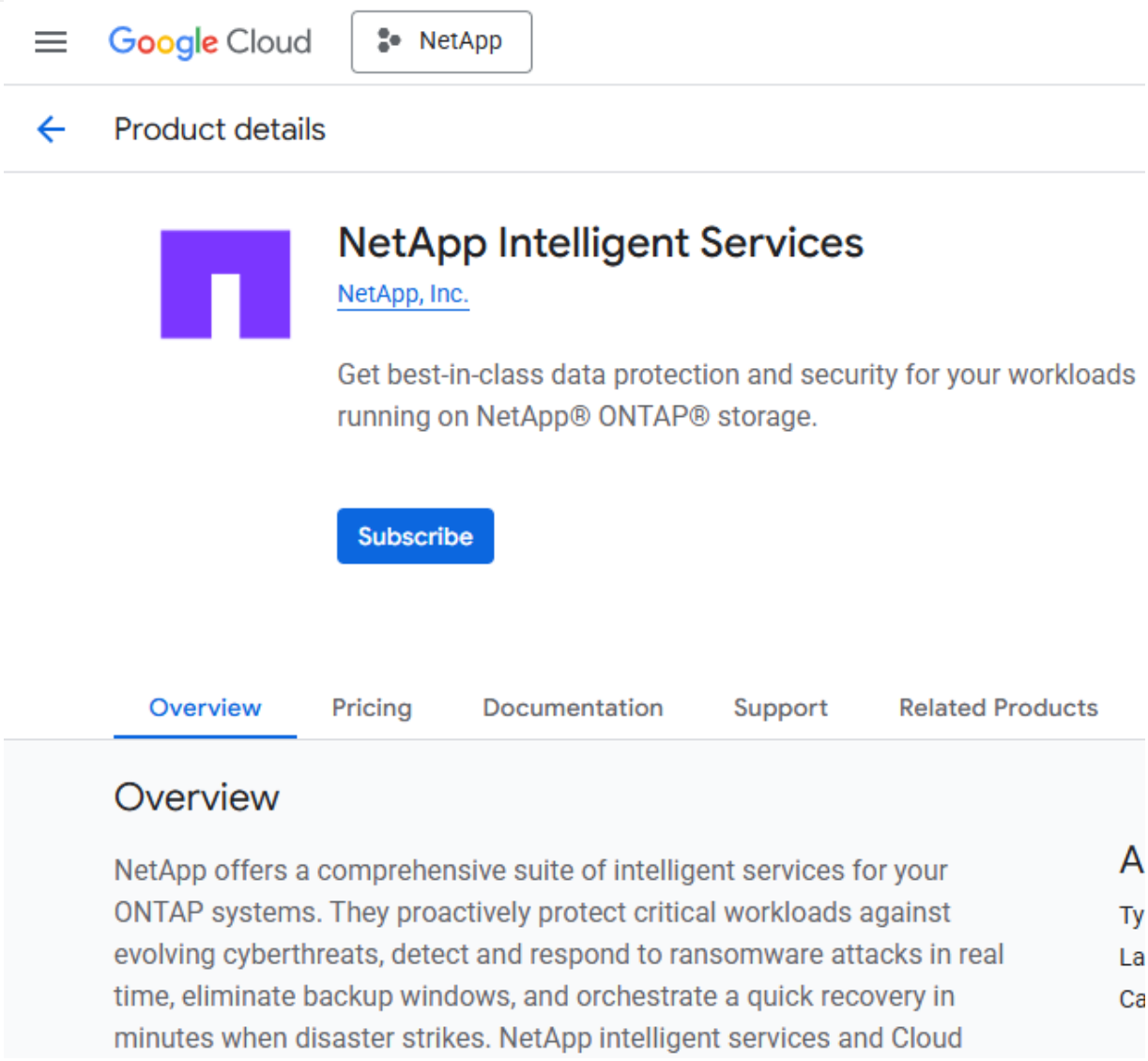
1. Para configurar una suscripción existente con las credenciales seleccionadas, seleccione un proyecto y una suscripción de Google Cloud de la lista desplegable y luego seleccione **Configurar**.



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.

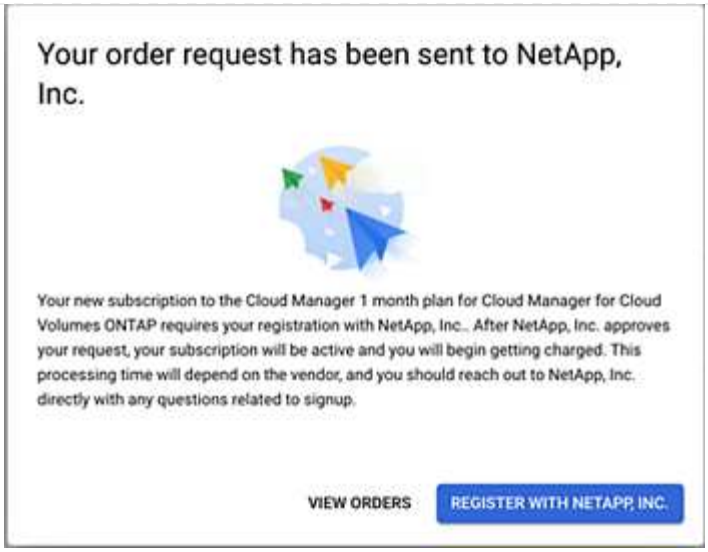


b. Seleccione **Suscribirse**.
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.
d. Seleccione **Suscribirse**.

   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.



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.

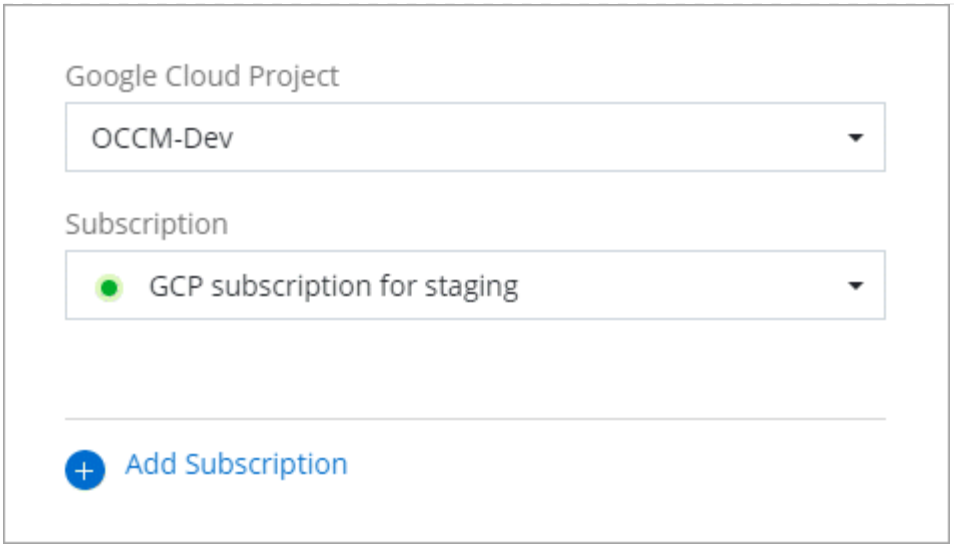
- Seleccione la organización de la consola con la que desea asociar esta suscripción.
- En el campo **Reemplazar suscripción existente**, elija si desea reemplazar automáticamente la suscripción existente de una organización con esta nueva suscripción.

  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"

Empieza con el modo privado

Flujo de trabajo de introducción (modo privado de BlueXP)

El modo privado de BlueXP (interfaz BlueXP heredada) generalmente se usa con entornos locales que no tienen conexión a Internet y con regiones de nube seguras, que incluyen AWS Secret Cloud, AWS Top Secret Cloud y Azure IL6. NetApp continúa brindando soporte a estos entornos con la interfaz BlueXP heredada.

"Documentación en PDF para el modo privado de BlueXP"

Funciones y servicios de datos compatibles con el modo privado

La siguiente tabla puede ayudarle a identificar rápidamente qué servicios y funciones de BlueXP son compatibles con el modo privado.

Tenga en cuenta que algunos servicios podrían ser compatibles con limitaciones.

Área de productos	Servicio o función de BlueXP	Modo privado
Entornos de trabajo Esta parte de la tabla enumera el soporte para la gestión del entorno de trabajo desde el lienzo de BlueXP . No indica los destinos de copia de seguridad admitidos para la BlueXP backup and recovery.	Amazon FSx para ONTAP	No
	Amazon S3	No
	Blob de Azure	No
	Azure NetApp Files	No
	Cloud Volumes ONTAP	Sí
	Google Cloud NetApp Volumes	No
	Almacenamiento en la nube de Google	No
	Clústeres ONTAP locales	Sí
	Serie E	No
	StorageGRID	No

Área de productos	Servicio o función de BlueXP	Modo privado
Servicios	Alertas	No
	Copia de seguridad y recuperación	Síhttps://docs.netapp.com/us-en/data-services-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["Ver la lista de destinos de respaldo admitidos para los datos de volumen de ONTAP"^]
	Clasificación	Sí
	Copiar y sincronizar	No
	Asesor digital	No
	Monedero digital	Sí
	Recuperación ante desastres	No
	Eficiencia económica	No
	Resiliencia frente al ransomware	No
	Replicación	Sí
	Actualizaciones de software	No
	Sostenibilidad	No
	Nivelación	No
	Almacenamiento en caché de volumen	No
	Fábrica de carga de trabajo	No
Características	Gestión de identidad y acceso	Sí
	Cartas credenciales	Sí
	Federación	No
	Autenticación multifactor	No
	Cuentas NSS	No
	Notificaciones	No
	Buscar	No
	Cronología	Sí