Agentes de consola

NetApp Console setup and administration

NetApp
January 27, 2026

Tabla de contenidos

Agentes de consola

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

	Disponible con agente	Disponible sin agente
Sistemas StorageGRID	Sí	No
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.

Implementar un agente de consola

AWS

Opciones de instalación del agente de consola en AWS

Hay algunas formas diferentes de crear un agente de consola en AWS. La forma más común es hacerlo directamente desde la NetApp Console .

Están disponibles las siguientes opciones de instalación:

- "Cree el agente de la consola directamente desde la consola"(esta es la opción estándar)

  Esta acción inicia una instancia EC2 que ejecuta Linux y el software del agente de consola en una VPC de su elección.

- "Cree un agente de consola desde AWS Marketplace"

  Esta acción también inicia una instancia EC2 que ejecuta Linux y el software del agente de consola, pero la implementación se inicia directamente desde AWS Marketplace, en lugar de desde la consola.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará su forma de prepararse para la instalación. Esto incluye cómo proporcionar a la consola los permisos necesarios para autenticar y administrar recursos en AWS.

Cree un agente de consola en AWS desde la NetApp Console

Puede crear un agente de consola en AWS directamente desde la NetApp Console. Antes de crear un agente de consola en AWS desde la consola, debe configurar su red y preparar los permisos de AWS.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .
- Deberías revisarlo"Limitaciones del agente de consola" .

Paso 1: Configurar la red para implementar un agente de consola en AWS

Asegúrese de que la ubicación de red donde planea instalar el agente de consola admita los siguientes requisitos. Estos requisitos permiten que el agente de la consola administre recursos y procesos en su nube híbrida.

VPC y subred

Cuando crea el agente de consola, debe especificar la VPC y la subred donde debe residir.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
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 .

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.

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.

Puntos finales contactados desde la consola de NetApp

A medida que utiliza la NetApp Console basada en web que se proporciona a través de la capa SaaS, esta se comunica con varios puntos finales para completar tareas de administración de datos. Esto incluye los puntos finales que se contactan para implementar el agente de la consola desde la consola.

"Ver la lista de puntos finales contactados desde la consola de NetApp" .

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"

Necesitará implementar este requisito de red después de crear el agente de consola.

Paso 2: Configurar los permisos de AWS para el agente de la consola

La consola debe autenticarse con AWS antes de poder implementar el agente de la consola en su VPC. Puede elegir uno de estos métodos de autenticación:

- Deje que la consola asuma un rol de IAM que tenga los permisos necesarios
- Proporcionar una clave de acceso de AWS y una clave secreta para un usuario de IAM que tenga los permisos necesarios

Con cualquiera de las opciones, el primer paso es crear una política de IAM. Esta política contiene solo los permisos necesarios para iniciar el agente de la consola en AWS desde la consola.

Si es necesario, puede restringir la política de IAM mediante el IAM `Condition` elemento. "Documentación de AWS: Elemento de condición"

Pasos

1. Vaya a la consola de AWS IAM.
2. Seleccione **Políticas > Crear política**.
3. Seleccione **JSON**.
4. Copie y pegue la siguiente política:

   Esta política contiene solo los permisos necesarios para iniciar el agente de la consola en AWS desde la consola. Cuando la consola crea el agente de consola, aplica un nuevo conjunto de permisos al agente de consola que le permite administrar los recursos de AWS. "Ver los permisos necesarios para el propio agente de la consola".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
```

```
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
```

```
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. Seleccione **Siguiente** y agregue etiquetas, si es necesario.
6. Seleccione **Siguiente** e ingrese un nombre y una descripción.
7. Seleccione **Crear política**.
8. Adjunte la política a un rol de IAM que la consola pueda asumir o a un usuario de IAM para poder proporcionar a la consola claves de acceso:
   - (Opción 1) Configure un rol de IAM que la consola pueda asumir:
     i. Vaya a la consola de AWS IAM en la cuenta de destino.
     ii. En Administración de acceso, seleccione **Roles > Crear rol** y siga los pasos para crear el rol.
     iii. En **Tipo de entidad confiable**, seleccione **Cuenta AWS**.
     iv. Seleccione **Otra cuenta de AWS** e ingrese el ID de la cuenta SaaS de la consola: 952013314444
     v. Seleccione la política que creó en la sección anterior.
     vi. Después de crear el rol, copie el ARN del rol para poder pegarlo en la consola cuando cree el agente de la consola.
   - (Opción 2) Configure permisos para un usuario de IAM para que pueda proporcionar a la consola claves de acceso:
     i. Desde la consola de AWS IAM, seleccione **Usuarios** y luego seleccione el nombre de usuario.
     ii. Seleccione **Agregar permisos > Adjuntar políticas existentes directamente**.
     iii. Seleccione la política que ha creado.
     iv. Seleccione **Siguiente** y luego seleccione **Agregar permisos**.
     v. Asegúrese de tener la clave de acceso y la clave secreta del usuario de IAM.

Resultado

Ahora debería tener un rol de IAM que tenga los permisos necesarios o un usuario de IAM que tenga los permisos necesarios. Al crear el agente de la consola desde la consola, puede proporcionar información sobre el rol o las claves de acceso.

Paso 3: Crear el agente de consola

Cree el agente de consola directamente desde la consola web.

Acerca de esta tarea

- Al crear el agente de la consola desde la consola, se implementa una instancia EC2 en AWS utilizando una configuración predeterminada. No cambie a una instancia EC2 más pequeña con menos CPU o menos RAM después de crear el agente de consola. "Obtenga información sobre la configuración predeterminada para el agente de la consola" .
- Cuando la consola crea el agente de consola, crea un rol de IAM y un perfil para el agente. Esta función incluye permisos que permiten al agente de la consola administrar los recursos de AWS. Asegúrese de que la función se actualice a medida que se agreguen nuevos permisos en futuras versiones. "Obtenga más información sobre la política de IAM para el agente de consola".

Antes de empezar

Debes tener lo siguiente:

- Un método de autenticación de AWS: un rol de IAM o claves de acceso para un usuario de IAM con los permisos requeridos.
- Una VPC y una subred que cumple con los requisitos de red.
- Un par de claves para la instancia EC2.
- Detalles sobre un servidor proxy, si se requiere un proxy para el acceso a Internet desde el agente de la consola.
- Configuración"requisitos de red" .
- Configuración"Permisos de AWS" .

Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione **Implementar agente > AWS**
3. Siga los pasos del asistente para crear el agente de consola:
4. En la página **Introducción** se ofrece una descripción general del proceso.
5. En la página **Credenciales de AWS**, especifique su región de AWS y luego elija un método de autenticación, que puede ser un rol de IAM que la consola puede asumir o una clave de acceso y una clave secreta de AWS.

   Si elige **Asumir rol**, puede crear el primer conjunto de credenciales desde el asistente de implementación del agente de la consola. Cualquier conjunto adicional de credenciales debe crearse desde la página Credenciales. Luego estarán disponibles en una lista desplegable del asistente. "Aprenda cómo agregar credenciales adicionales" .

6. En la página **Detalles**, proporcione detalles sobre el agente de consola.
   - Introduzca un nombre.
   - Añadir etiquetas personalizadas (metadatos).

- Elija si desea que la Consola cree un nuevo rol que tenga los permisos necesarios o si desea seleccionar un rol existente que haya configurado con"los permisos requeridos" .
- Elija si desea cifrar los discos EBS del agente de consola. Tiene la opción de utilizar la clave de cifrado predeterminada o utilizar una clave personalizada.

7. En la página **Red**, especifique una VPC, una subred y un par de claves para el agente, elija si desea habilitar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.

   Asegúrese de tener el par de claves correcto para acceder a la máquina virtual del agente de consola. Sin un par de claves, no puedes acceder a él.

8. En la página **Grupo de seguridad**, elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita las reglas de entrada y salida requeridas.

   "Ver las reglas del grupo de seguridad para AWS" .

9. Revise sus selecciones para verificar que su configuración sea correcta.

   a. La casilla de verificación **Validar configuración del agente** está marcada de forma predeterminada para que la consola valide los requisitos de conectividad de red cuando se implementa. Si la consola no logra implementar el agente, proporciona un informe para ayudarlo a solucionar el problema. Si la implementación se realiza correctamente, no se proporciona ningún informe.

   Si todavía estás usando el"puntos finales anteriores" utilizado para actualizaciones de agente, la validación falla con un error. Para evitar esto, desmarque la casilla de verificación para omitir la comprobación de validación.

10. Seleccione **Agregar**.

    La consola implementa el agente en aproximadamente 10 minutos. Permanezca en la página hasta que se complete el proceso.

Resultado

Una vez completado el proceso, el agente de la consola estará disponible para su uso desde la consola.

Si la implementación falla, puedes descargar un informe y registros desde la Consola para ayudarte a solucionar los problemas."Aprenda a solucionar problemas de instalación."

Si tiene depósitos de Amazon S3 en la misma cuenta de AWS donde creó el agente de consola, verá aparecer automáticamente un entorno de trabajo de Amazon S3 en la página **Sistemas**. "Aprenda a administrar los buckets S3 desde la NetApp Console"

Cree un agente de consola desde AWS Marketplace

Puede crear un agente de consola en AWS directamente desde AWS Marketplace. Para crear un agente de consola desde AWS Marketplace, debe configurar su red, preparar los permisos de AWS, revisar los requisitos de la instancia y luego crear el agente de consola.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .

- Deberías revisarlo"Limitaciones del agente de consola" .

Paso 1: Configurar la red

Asegúrese de que la ubicación de red del agente de la consola cumpla con los siguientes requisitos para administrar los recursos de la nube híbrida.

VPC y subred

Cuando crea el agente de consola, debe especificar la VPC y la subred donde debe residir.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
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 .
\ https://mysupport.netapp.com	Para obtener información de licencias y enviar mensajes de AutoSupport al soporte de NetApp .

Puntos finales	Objetivo
\ 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.

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"

Implemente este acceso a la red después de crear el agente de consola.

Paso 2: Configurar los permisos de AWS

Para prepararse para una implementación de mercado, cree políticas de IAM en AWS y adjúntelas a una función de IAM. Cuando crea el agente de consola desde AWS Marketplace, se le solicita que seleccione esa función de IAM.

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.

      Es posible que necesite crear una segunda política basada en los servicios de datos de NetApp que planea utilizar. 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. 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 que puede asociar con la instancia EC2 durante la implementación desde AWS Marketplace.

Paso 3: Revisar los requisitos de la instancia

Al crear el agente de consola, debe elegir un tipo de instancia EC2 que cumpla con los siguientes requisitos.

UPC

8 núcleos u 8 vCPU

RAM

32 GB

Tipo de instancia de AWS EC2

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

Paso 4: Crear el agente de consola

Cree el agente de consola directamente desde AWS Marketplace.

Acerca de esta tarea

Al crear el agente de consola desde AWS Marketplace, se implementa una instancia EC2 en AWS utilizando una configuración predeterminada. "Obtenga información sobre la configuración predeterminada para el agente de la consola" .

Antes de empezar

Debes tener lo siguiente:

- Una VPC y una subred que cumple con los requisitos de red.
- Una función de IAM con una política adjunta que incluye los permisos necesarios para el agente de la consola.
- 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 la instancia.
- 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**.

     AWS inicia el agente de consola con la configuración especificada y el agente de consola se ejecuta en aproximadamente diez minutos.

   Si la instalación falla, puede ver registros y un informe para ayudarlo a solucionar problemas."Aprenda a solucionar problemas de instalación."

8. Abra un navegador web desde un host que tenga una conexión a la máquina virtual del agente de consola y la URL del agente de consola.
9. Después de iniciar sesión, configure el agente de la consola:
   a. Especifique la organización de la consola que se asociará con el agente de la consola.
   b. Introduzca un nombre para el sistema.
   c. En **¿Está ejecutando en un entorno seguro?** mantenga el modo restringido deshabilitado.

Mantenga el modo restringido deshabilitado para utilizar la consola en modo estándar. Debe habilitar el modo restringido solo si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de backend de la consola. Si ese es el caso,"Siga los pasos para comenzar a utilizar la NetApp Console en modo restringido" .

d. Seleccione **Comencemos**.

Resultado

El agente de consola ahora está instalado y configurado con su organización de consola.

Abra un navegador web y vaya a "NetApp Console" para comenzar a utilizar el agente de la consola con la consola.

Si tiene depósitos de Amazon S3 en la misma cuenta de AWS donde creó el agente de consola, verá aparecer automáticamente un entorno de trabajo de Amazon S3 en la página **Sistemas**. "Aprenda a administrar los buckets S3 desde la NetApp Console"

Instalar manualmente el agente de consola en AWS

Puede instalar manualmente un agente de consola en un host Linux que se ejecute en AWS. Para instalar manualmente el agente de consola en su propio host Linux, debe revisar los requisitos del host, configurar su red, preparar los permisos de AWS, instalar el agente de consola y luego proporcionar los permisos que preparó.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .
- Deberías revisarlo"Limitaciones del agente de consola" .

Paso 1: Revisar los requisitos del host

Asegúrese de que el host que ejecuta el software del agente de consola cumpla con los requisitos del sistema operativo, RAM y puerto.

> El agente de consola reserva el rango de UID y GID de 19000 a 19200. Este rango es fijo y no se puede modificar. Si algún software de terceros en su host utiliza UID o GID dentro de este rango, la instalación del agente fallará. NetApp recomienda utilizar un host que esté libre de software de terceros para evitar conflictos.

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.

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 .

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
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 .
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 .

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Compatible con modo de aplicación o modo permisivo	Ubuntu		24,04 LTS	3.9.45 o posterior con la NetApp Console en modo estándar o modo restringido
Motor Docker 23.06 a 28.0.0.	No compatible		22,04 LTS	3.9.50 o posterior

Par de claves

Cuando cree el agente de consola, deberá seleccionar un par de claves EC2 para usar con la instancia.

Límite de salto de respuesta PUT al usar IMDSv2

Si IMDSv2 está habilitado (el valor predeterminado para las nuevas instancias de EC2), establezca el límite de saltos de respuesta PUT en 3. Si no lo hace, el sistema muestra un error de inicialización de la interfaz de usuario durante la configuración del agente.

- "Requerir el uso de IMDSv2 en instancias de Amazon EC2"
- "Documentación de AWS: Cambiar el límite de saltos de respuesta PUT"

Paso 2: Instalar 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 3: Configurar la red

Asegúrese de que la ubicación de la red admita los siguientes requisitos para que el agente de la consola pueda administrar recursos en su nube híbrida.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde computadoras al usar la NetApp Console basada en web

Las computadoras que acceden a la consola desde un navegador web deben tener la capacidad de comunicarse con varios puntos finales. Necesitará usar la consola para configurar el agente de la consola y para el uso diario de la consola.

"Preparar la red para la consola de NetApp" .

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
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 .
\ https://mysupport.netapp.com	Para obtener información de licencias y enviar mensajes de AutoSupport al soporte de NetApp .

Puntos finales	Objetivo
\ 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.

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"

Paso 4: Configurar los permisos de AWS para la consola

Proporcione permisos de AWS a la NetApp Console mediante una de estas opciones:

- Opción 1: Cree políticas de IAM y adjúntelas a un rol de IAM que pueda asociar con la instancia EC2.
- Opción 2: proporcionar a la consola la clave de acceso de AWS para un usuario de IAM que tenga los permisos necesarios.

Siga los pasos para preparar los permisos para la consola.

Rol de IAM

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. 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 una función de IAM que puede asociar con la instancia EC2 después de instalar el agente de consola.

Clave de acceso de AWS

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.

Resultado

Ahora tiene un usuario IAM que tiene los permisos necesarios y una clave de acceso que puede proporcionar a la consola.

Paso 5: Instalar el agente de consola

Después de completar los requisitos previos, instale manualmente el software en su host Linux.

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".

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.

2. Espere a que se complete la instalación.

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

   Si la instalación falla, puede ver el informe de instalación y los registros para ayudarlo a solucionar los problemas."Aprenda a solucionar problemas de instalación."

1. Abra un navegador web desde un host que tenga una conexión a la máquina virtual del agente de consola e ingrese la siguiente URL:

   https://ipaddress

2. Después de iniciar sesión, configure el agente de la consola:

   a. Especifique la organización que se asociará con el agente de la consola.

   b. Introduzca un nombre para el sistema.

   c. En **¿Está ejecutando en un entorno seguro?** mantenga el modo restringido deshabilitado.

      Debes mantener el modo restringido deshabilitado porque estos pasos describen cómo usar la consola en modo estándar. Debe habilitar el modo restringido solo si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de backend. Si ese es el caso,"Siga los pasos para comenzar a utilizar la NetApp Console en modo restringido" .

   d. Seleccione **Comencemos**.

Si tiene depósitos de Amazon S3 en la misma cuenta de AWS donde creó el agente de consola, verá aparecer automáticamente un sistema de almacenamiento de Amazon S3 en la página **Sistemas**. "Aprenda a administrar los buckets S3 desde NetApp ConsoleP"

Paso 6: Proporcionar permisos a la NetApp Console

Después de instalar el agente de consola, proporcione los permisos de AWS que configuró para que el agente de consola pueda administrar sus datos y su infraestructura de almacenamiento en AWS.

Rol de IAM

Adjunte la función de IAM que cree a la instancia EC2 del agente de consola.

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**.

Ir a la "NetApp Console" para comenzar a utilizar el agente de consola.

Clave de acceso de AWS

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

Pasos

1. Asegúrese de que el agente de consola correcto esté seleccionado actualmente en la consola.
2. Seleccione **Administración > Credenciales**.
3. Seleccione **Credenciales de la organización**.
4. 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**.

Ir a la "NetApp Console" para comenzar a utilizar el agente de consola.

Azur

Opciones de instalación del agente de consola en Azure

Hay algunas formas diferentes de crear un agente de consola en Azure. La forma más común es hacerlo directamente desde la NetApp Console .

Están disponibles las siguientes opciones de instalación:

- "Cree un agente de consola directamente desde la NetApp Console"(esta es la opción estándar)

  Esta acción inicia una máquina virtual que ejecuta Linux y el software del agente de consola en una red virtual de su elección.

- "Crear un agente de consola desde Azure Marketplace"

  Esta acción también inicia una máquina virtual que ejecuta Linux y el software del agente de consola, pero la implementación se inicia directamente desde Azure Marketplace, en lugar de desde la consola.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará su forma de prepararse para la instalación. Esto incluye cómo proporcionar al agente de consola los permisos necesarios para autenticar y administrar recursos en Azure.

Crear un agente de consola en Azure desde la NetApp Console

Para crear un agente de consola en Azure desde la NetApp Console, debe configurar su red, preparar los permisos de Azure y luego crear el agente de consola.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .
- Deberías revisarlo"Limitaciones del agente de consola" .

Paso 1: Configurar la red

Asegúrese de que la ubicación de red donde planea instalar el agente de consola admita los siguientes requisitos. Estos requisitos permiten que el agente de la consola administre recursos de nube híbrida.

Región de Azure

Si usa Cloud Volumes ONTAP, el agente de la consola debe implementarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que administra, o en la "Par de regiones de Azure" para los sistemas Cloud Volumes ONTAP . Este requisito 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"

VNet y subred

Al crear el agente de consola, debe especificar la red virtual y la subred donde debe residir.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
\ 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.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para administrar recursos en las regiones de Azure China.
\ 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.

Puntos finales contactados desde la consola de NetApp

A medida que utiliza la NetApp Console basada en web que se proporciona a través de la capa SaaS, esta se comunica con varios puntos finales para completar tareas de administración de datos. Esto incluye los puntos finales que se contactan para implementar el agente de la consola desde la consola.

"Ver la lista de puntos finales contactados desde la consola de NetApp" .

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"

Debe implementar este requisito de red después de crear el agente de consola.

Paso 2: Crear una política de implementación del agente de consola (función personalizada)

Debe crear un rol personalizado que tenga permisos para implementar el agente de consola en Azure.

Cree un rol personalizado de Azure que pueda asignar a su cuenta de Azure o a una entidad de servicio de Microsoft Entra. La consola se autentica con Azure y utiliza estos permisos para crear el agente de la consola en su nombre.

La consola implementa la máquina virtual del agente de consola en Azure y habilita una "identidad administrada asignada por el sistema" , crea el rol requerido y lo asigna a la VM. "Revisar cómo la Consola utiliza los permisos" .

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. Copie los permisos necesarios para un nuevo rol personalizado en Azure y guárdelos en un archivo JSON.

   Esta función personalizada contiene solo los permisos necesarios para iniciar la máquina virtual del agente de consola en Azure desde la consola. No utilice esta política para otras situaciones. Cuando la consola crea el agente de consola, aplica un nuevo conjunto de permisos a la máquina virtual del agente de consola que le permite administrar los recursos de Azure.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
```

```
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
```

```
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Azure SetupAsService",
  "IsCustom": "true"
}
```

2. Modifique el JSON agregando su identificador de suscripción de Azure al ámbito asignable.

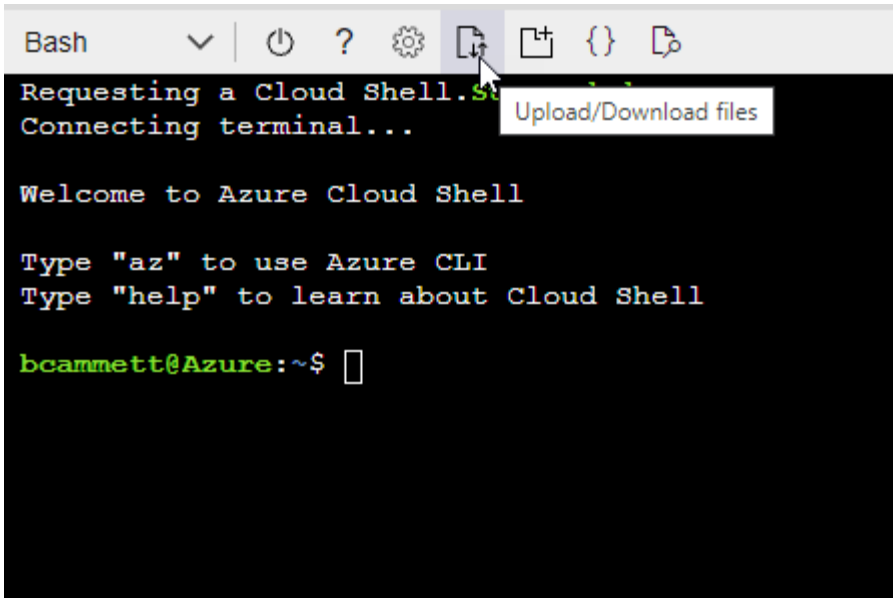
   Ejemplo

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

3. 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. Ingrese el siguiente comando CLI de Azure:

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

Ahora tiene un rol personalizado llamado *Azure SetupAsService*. Puede aplicar esta función personalizada a su cuenta de usuario o a una entidad de servicio.

Paso 3: Configurar la autenticación

Al crear el agente de la consola desde la consola, debe proporcionar un inicio de sesión que permita que la consola se autentique con Azure e implemente la máquina virtual. Tienes dos opciones:

1. Sign in con su cuenta de Azure cuando se le solicite. Esta cuenta debe tener permisos específicos de Azure. Esta es la opción predeterminada.
2. Proporcionar detalles sobre una entidad de servicio de Microsoft Entra. Esta entidad de servicio también requiere permisos específicos.

Siga los pasos para preparar uno de estos métodos de autenticación para usar con la consola.

Cuenta de Azure

Asigne el rol personalizado al usuario que implementará el agente de la consola desde la consola.

Pasos

1. En el portal de Azure, abra el servicio **Suscripciones** y seleccione la suscripción del usuario.
2. Haga clic en **Control de acceso (IAM)**.
3. Haga clic en **Agregar** > **Agregar asignación de rol** y luego agregue los permisos:
   a. Seleccione la función **Azure SetupAsService** y haga clic en **Siguiente**.

   > Azure SetupAsService es el nombre predeterminado proporcionado en la política de implementación del agente de consola para Azure. Si eligió un nombre diferente para el rol, seleccione ese nombre en su lugar.

   b. Mantenga seleccionado **Usuario, grupo o entidad de servicio**.
   c. Haga clic en **Seleccionar miembros**, elija su cuenta de usuario y haga clic en **Seleccionar**.
   d. Haga clic en **Siguiente**.
   e. Haga clic en **Revisar + asignar**.

Director de servicio

En lugar de iniciar sesión con su cuenta de Azure, puede proporcionar a la consola las credenciales de una entidad de servicio de Azure que tenga los permisos necesarios.

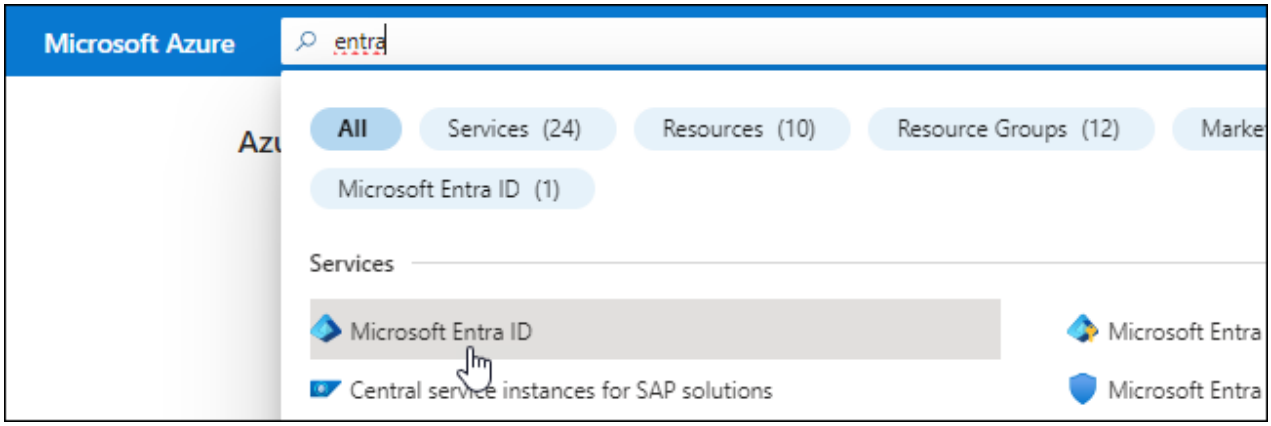
Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita la consola.

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**.

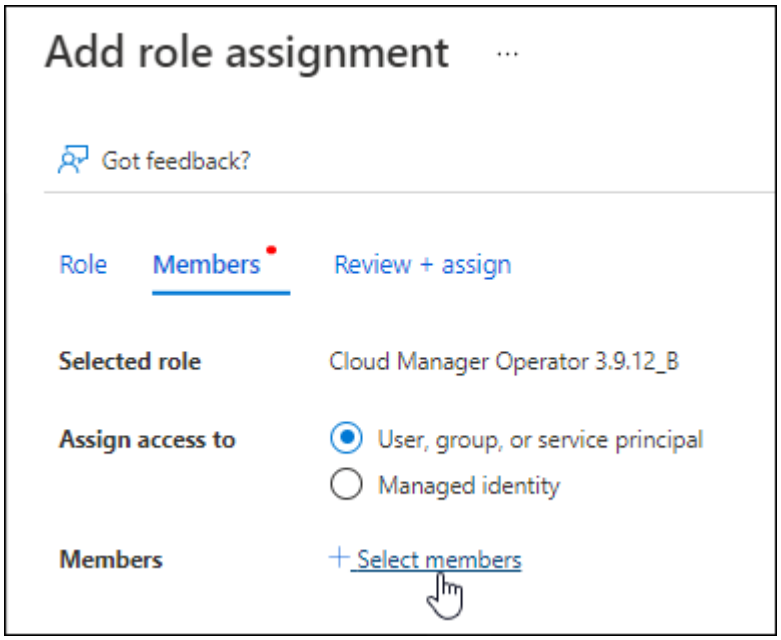
   Ha creado la aplicación AD y la entidad principal de servicio.

Asignar el rol personalizado a la aplicación

1. Desde el portal de Azure, abra el servicio **Suscripciones**.
2. Seleccione la suscripción.
3. Haga clic en **Control de acceso (IAM) > Agregar > Agregar asignación de rol**.
4. En la pestaña **Rol**, seleccione el rol **Operador de consola** y haga clic en **Siguiente**.
5. En la pestaña **Miembros**, complete los siguientes pasos:

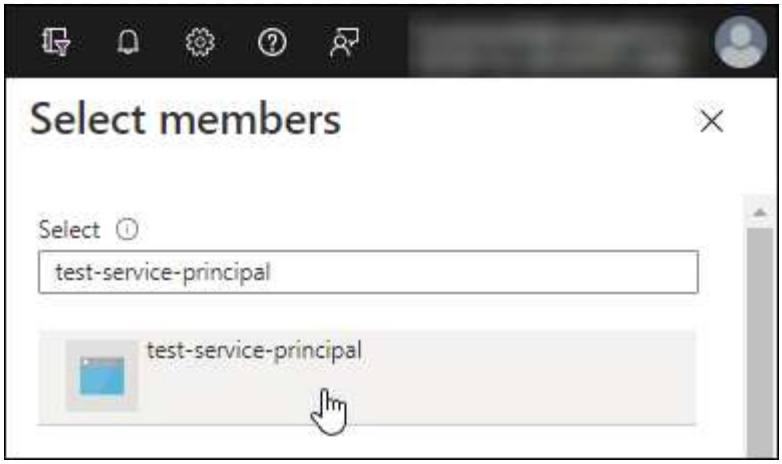
   a. Mantenga seleccionado **Usuario, grupo o entidad de servicio**.

   b. Haga clic en **Seleccionar miembros**.



   c. Busque el nombre de la aplicación.

   He aquí un ejemplo:



a. Seleccione la aplicación y haga clic en **Seleccionar**.

b. Haga clic en **Siguiente**.

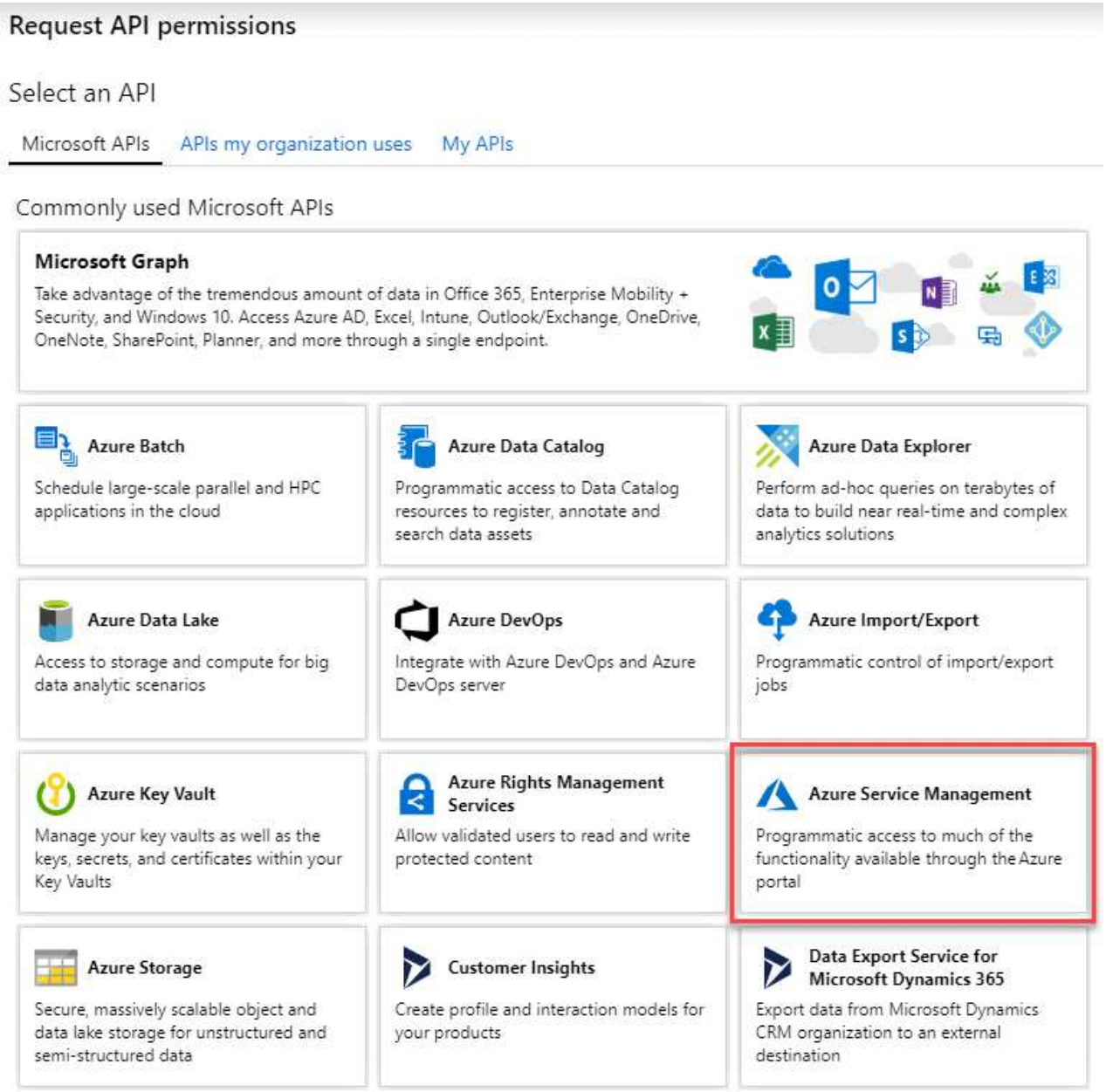
6. Haga clic en **Revisar + asignar**.

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

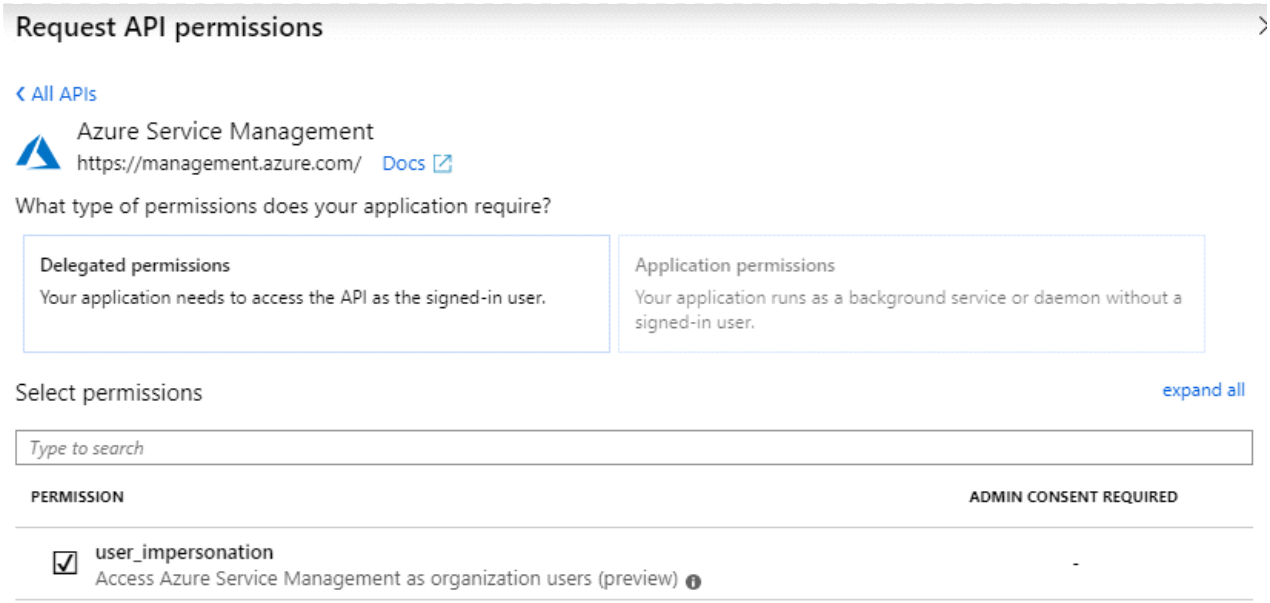
   Si desea administrar recursos en varias suscripciones de Azure, debe vincular la entidad de servicio a cada una de esas suscripciones. Por ejemplo, la consola le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

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**.

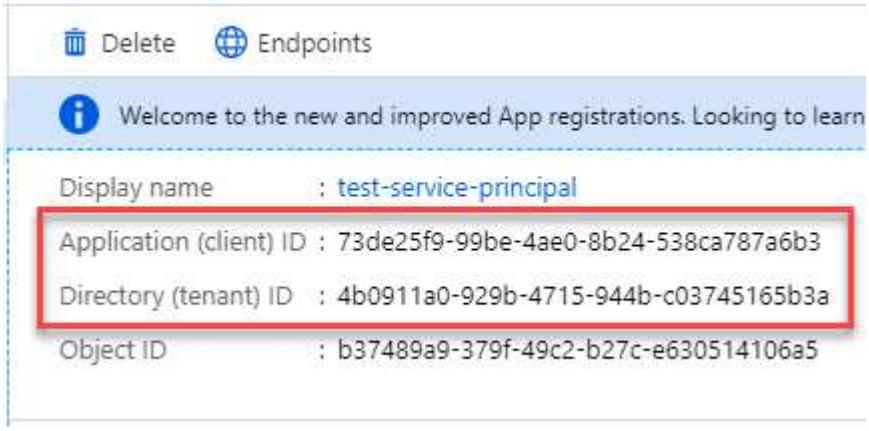


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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 crea el agente de Consola.

Paso 4: Crear el agente de consola

Cree el agente de consola directamente desde la NetApp Console.

Acerca de esta tarea

- Al crear el agente de consola desde la consola, se implementa una máquina virtual en Azure utilizando una configuración predeterminada. No cambie a una instancia de VM más pequeña con menos CPU o menos RAM después de crear el agente de consola. "Obtenga información sobre la configuración predeterminada para el agente de la consola" .
- Cuando la consola implementa el agente de la consola, crea un rol personalizado y lo asigna a la máquina virtual del agente de la consola. Esta función incluye permisos que permiten al agente de consola administrar recursos de Azure. Debe asegurarse de que la función se mantenga actualizada a medida que se agreguen nuevos permisos en versiones posteriores. "Obtenga más información sobre el rol personalizado para el agente de consola" .

Antes de empezar

Debes tener lo siguiente:

- Una suscripción de Azure.
- Una red virtual y una subred en la región de Azure que elija.
- Detalles sobre un servidor proxy, si su organización requiere un proxy para todo el tráfico de Internet saliente:
  - Dirección IP
  - Cartas credenciales
  - Certificado HTTPS
- Una clave pública SSH, si desea utilizar ese método de autenticación para la máquina virtual del agente de consola. La otra opción para el método de autenticación es utilizar una contraseña.

  "Obtenga información sobre cómo conectarse a una máquina virtual Linux en Azure"

- Si no desea que la consola cree automáticamente un rol de Azure para el agente de la consola, deberá crear el suyo propio."utilizando la política de esta página" .

  Estos permisos son para el propio agente de la consola. Es un conjunto de permisos diferente al que configuró previamente para implementar la máquina virtual del agente de consola.

Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione **Implementar agente > Azure**
3. En la página **Revisión**, revise los requisitos para implementar un agente. Estos requisitos también se detallan más arriba en esta página.
4. En la página **Autenticación de máquina virtual**, seleccione la opción de autenticación que coincida con cómo configura los permisos de Azure:

   - Seleccione **Iniciar sesión** para iniciar sesión en su cuenta Microsoft, que debería tener los permisos necesarios.

     El formulario es propiedad de Microsoft y está alojado por esta empresa. Sus credenciales no se proporcionan a NetApp.

     Si ya ha iniciado sesión en una cuenta de Azure, la consola usa automáticamente esa cuenta. Si tiene varias cuentas, es posible que primero deba cerrar la sesión para asegurarse de que está usando la cuenta correcta.

   - Seleccione **Entidad principal de servicio de Active Directory** para ingresar información sobre la entidad principal de servicio de Microsoft Entra que otorga los permisos necesarios:
     - ID de la aplicación (cliente)
     - ID de directorio (inquilino)
     - Secreto del cliente

   Aprenda cómo obtener estos valores para una entidad de servicio .

5. En la página **Autenticación de máquina virtual**, elija una suscripción de Azure, una ubicación, un nuevo grupo de recursos o un grupo de recursos existente y, luego, elija un método de autenticación para la máquina virtual del agente de consola que está creando.

   El método de autenticación para la máquina virtual puede ser una contraseña o una clave pública SSH.

   "Obtenga información sobre cómo conectarse a una máquina virtual Linux en Azure"

6. En la página **Detalles**, ingrese un nombre para el agente, especifique las etiquetas y elija si desea que la Consola cree un nuevo rol que tenga los permisos necesarios o si desea seleccionar un rol existente que configuró con"los permisos requeridos" .

   Tenga en cuenta que puede elegir las suscripciones de Azure asociadas con este rol. Cada suscripción que elija proporciona al agente de la consola permisos para administrar recursos en esa suscripción (por ejemplo, Cloud Volumes ONTAP).

7. En la página **Red**, elija una red virtual y una subred, si desea habilitar una dirección IP pública y, opcionalmente, especifique una configuración de proxy.

   - En la página **Grupo de seguridad**, elija si desea crear un nuevo grupo de seguridad o si desea seleccionar un grupo de seguridad existente que permita las reglas de entrada y salida requeridas.

     "Ver las reglas del grupo de seguridad para Azure" .

8. Revise sus selecciones para verificar que su configuración sea correcta.

a. La casilla de verificación **Validar configuración del agente** está marcada de forma predeterminada para que la consola valide los requisitos de conectividad de red cuando se implementa. Si la consola no logra implementar el agente, proporciona un informe para ayudarlo a solucionar el problema. Si la implementación se realiza correctamente, no se proporciona ningún informe.

Si todavía estás usando el"puntos finales anteriores" utilizado para actualizaciones de agente, la validación falla con un error. Para evitar esto, desmarque la casilla de verificación para omitir la comprobación de validación.

9. Seleccione **Agregar**.

La consola prepara al agente en aproximadamente 10 minutos. Permanezca en la página hasta que se complete el proceso.

Resultado

Una vez completado el proceso, el agente de la consola estará disponible para su uso desde la consola.

Si la implementación falla, puedes descargar un informe y registros desde la Consola para ayudarte a solucionar los problemas."Aprenda a solucionar problemas de instalación."

Si tiene Azure Blob Storage en la misma cuenta de Azure donde creó el agente de consola, verá que Azure Blob Storage aparece automáticamente en la página **Sistemas**. "Aprenda a administrar Azure Blob Storage desde la NetApp Console"

Crear un agente de consola desde Azure Marketplace

Puede crear un agente de consola en Azure directamente desde Azure Marketplace. Para crear un agente de consola desde Azure Marketplace, debe configurar su red, preparar los permisos de Azure, revisar los requisitos de la instancia y luego crear el agente de consola.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .
- Revisar"Limitaciones del agente de consola" .

Paso 1: Configurar la red

Asegúrese de que la ubicación de red donde planea instalar el agente de consola admita los siguientes requisitos. Estos requisitos permiten que el agente de consola administre recursos en su nube híbrida.

Región de Azure

Si usa Cloud Volumes ONTAP, el agente de la consola debe implementarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que administra, o en la "Par de regiones de Azure" para los sistemas Cloud Volumes ONTAP . Este requisito 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"

VNet y subred

Al crear el agente de consola, debe especificar la red virtual y la subred donde debe residir.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
\ 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.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para administrar recursos en las regiones de Azure China.
\ 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.

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"

Implemente los requisitos de red después de crear el agente de consola.

Paso 2: Revisar los requisitos de la máquina virtual

Al crear el agente de consola, elija un tipo de máquina virtual que cumpla con los siguientes requisitos.

UPC

8 núcleos u 8 vCPU

RAM

32 GB

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.

Paso 3: Configurar permisos

Puede proporcionar permisos de las siguientes maneras:

- Opción 1: Asignar un rol personalizado a la máquina virtual de Azure mediante una identidad administrada asignada por el sistema.
- Opción 2: proporcione a la consola las credenciales de una entidad de servicio de Azure que tenga los permisos necesarios.

Siga estos pasos para configurar permisos para la consola.

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"

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.

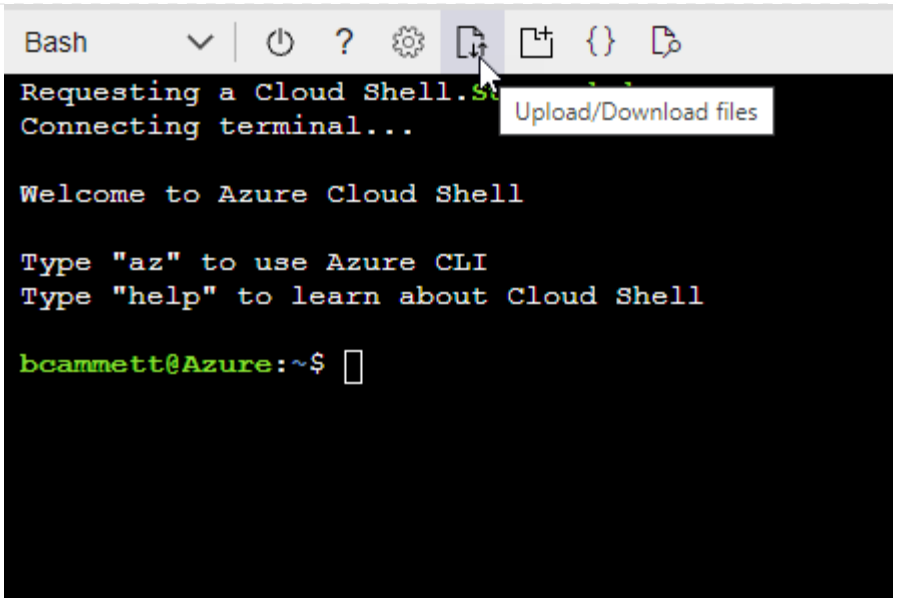
   Ejemplo

   ```
   "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
```

Director de servicio

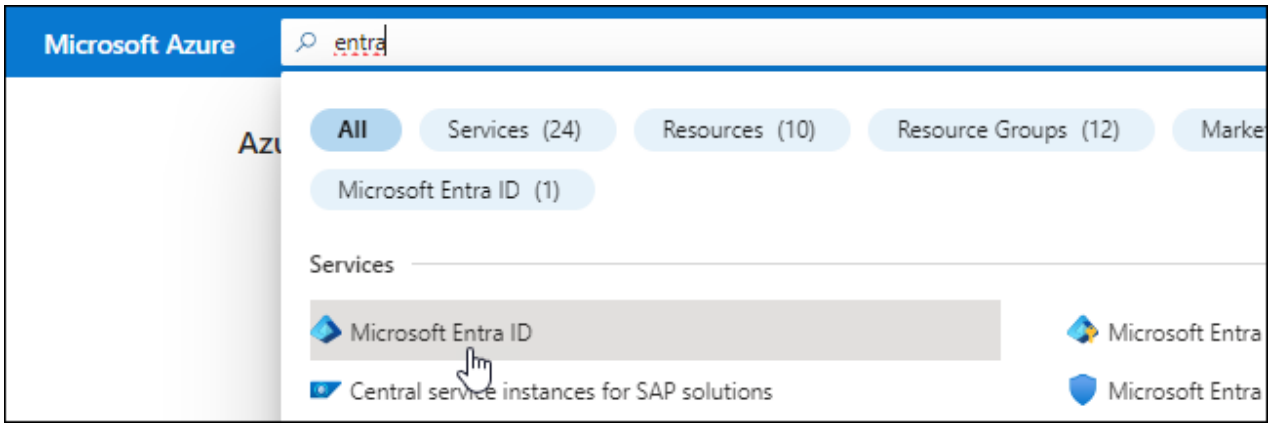
Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita la consola.

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 .

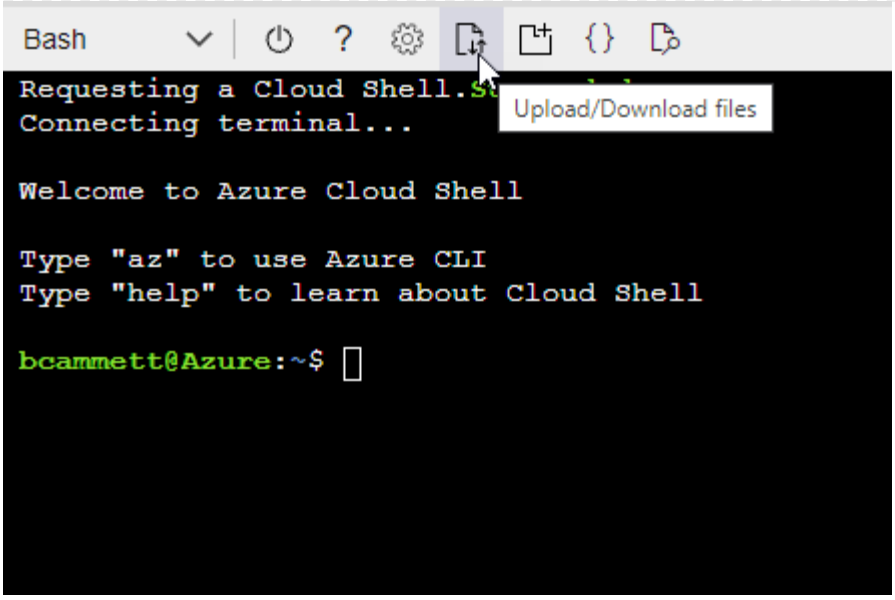
      Ejemplo

      ```
      "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**.

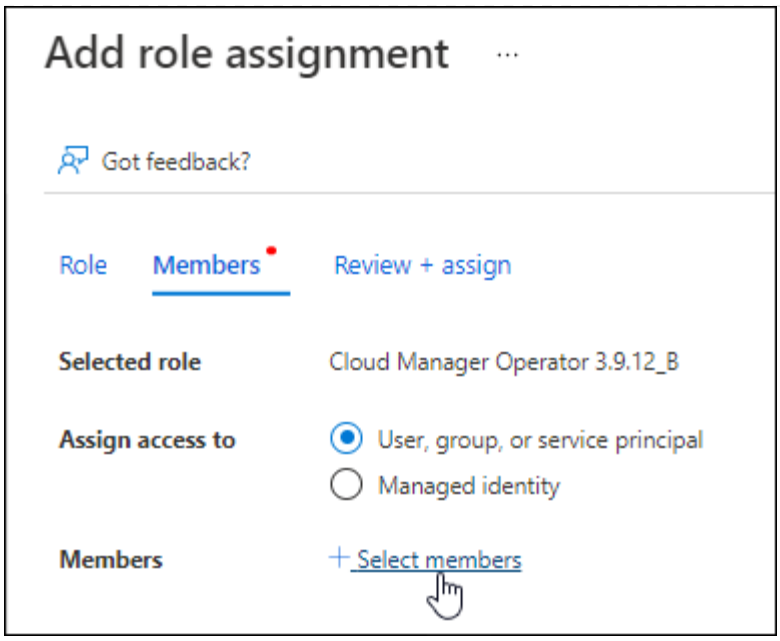
   b. Seleccione la suscripción.

   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**.

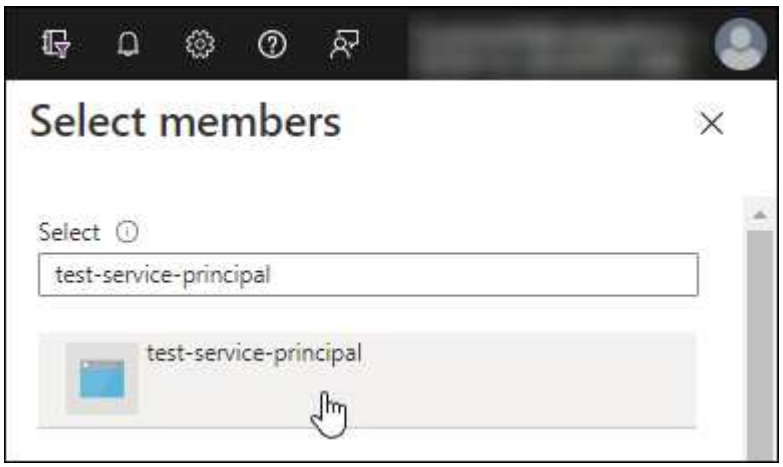
   e. En la pestaña **Miembros**, complete los siguientes pasos:

      - 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**.

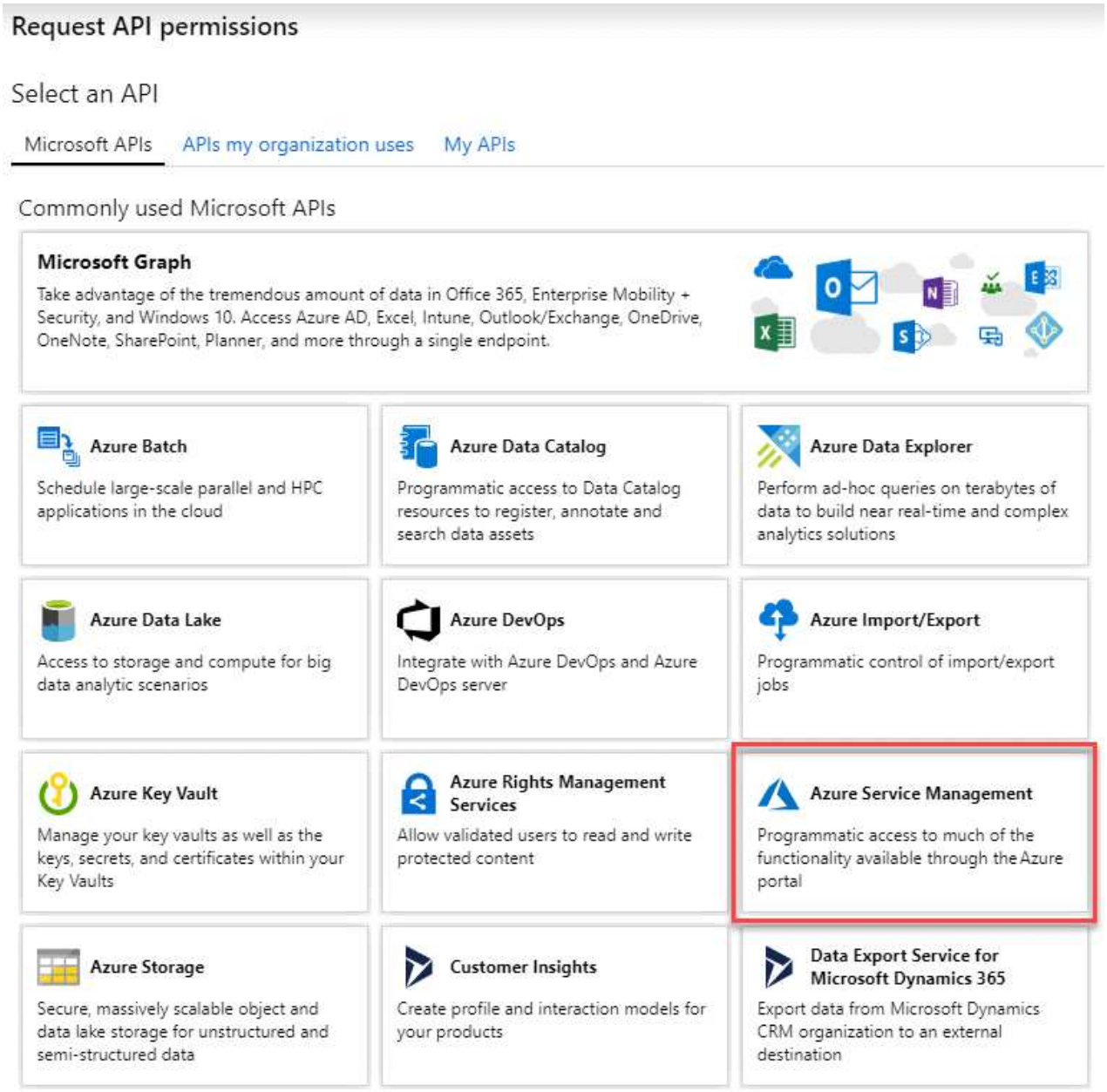
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

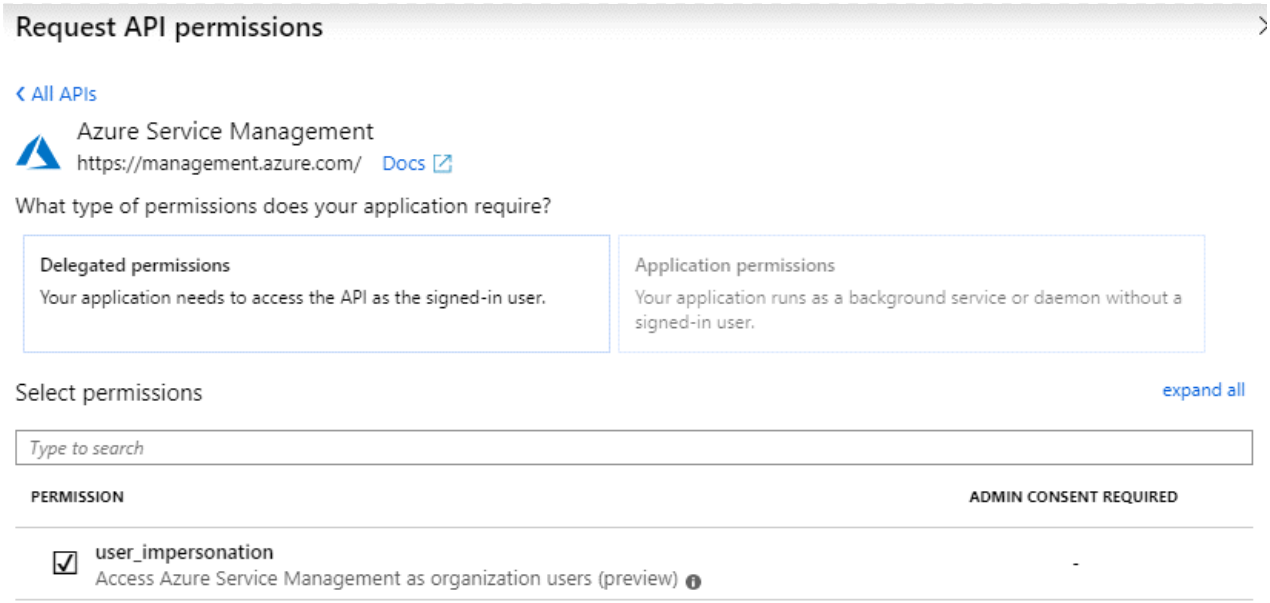
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

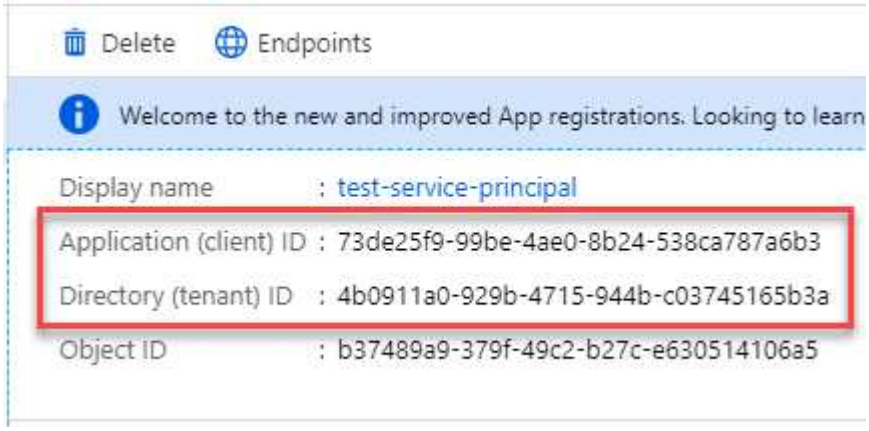


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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

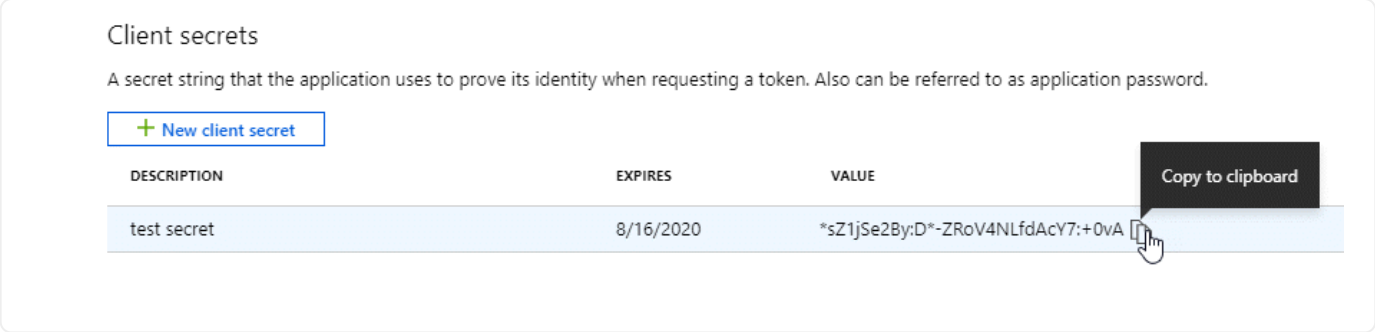
1. En el servicio **Microsoft Entra ID**, seleccione **Registros de aplicaciones** y seleccione la aplicación.
2. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)**.



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.



Paso 4: Crear el agente de consola

Inicie el agente de consola directamente desde Azure Marketplace.

Acerca de esta tarea

Al crear el agente de consola desde Azure Marketplace, se configura una máquina virtual con una configuración predeterminada. "Obtenga información sobre la configuración predeterminada para el agente de la consola" .

Antes de empezar

Debes tener lo siguiente:

- Una suscripción de Azure.
- Una red virtual y una subred en la región de Azure que elija.
- Detalles sobre un servidor proxy, si su organización requiere un proxy para todo el tráfico de Internet saliente:
  - Dirección IP
  - Cartas credenciales
  - Certificado HTTPS
- Una clave pública SSH, si desea utilizar ese método de autenticación para la máquina virtual del agente de consola. La otra opción para el método de autenticación es utilizar una contraseña.

  "Obtenga información sobre cómo conectarse a una máquina virtual Linux en Azure"

- Si no desea que la consola cree automáticamente un rol de Azure para el agente de la consola, deberá crear el suyo propio."utilizando la política de esta página" .

  Estos permisos son para la propia instancia del agente de consola. Es un conjunto de permisos diferente al que configuró previamente para implementar la máquina virtual del agente de consola.

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"

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.
- **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**.

  Esta configuración es importante porque una identidad administrada permite que la máquina virtual del agente de consola se identifique con Microsoft Entra ID sin proporcionar ninguna credencial. "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.

   Azure implementa la máquina virtual con la configuración especificada. Debería ver la máquina virtual y el software del agente de consola ejecutándose en aproximadamente diez minutos.

   Si la instalación falla, puede ver registros y un informe para ayudarlo a solucionar problemas."Aprenda a solucionar problemas de instalación."

5. Abra un navegador web desde un host que tenga una conexión a la máquina virtual del agente de consola e ingrese la siguiente URL:

   https://ipaddress

6. Después de iniciar sesión, configure el agente de la consola:
   a. Especifique la organización de la consola que se asociará con el agente de la consola.
   b. Introduzca un nombre para el sistema.
   c. En **¿Está ejecutando en un entorno seguro?** mantenga el modo restringido deshabilitado.

      Mantenga el modo restringido deshabilitado para utilizar la consola en modo estándar. Debe habilitar el modo restringido solo si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de backend de la consola. Si ese es el caso,"Siga los pasos para comenzar a utilizar la consola en modo restringido" .

   d. Seleccione **Comencemos**.

Resultado

Ahora ha instalado el agente de la consola y lo ha configurado con su organización de la consola.

Si tiene Azure Blob Storage en la misma suscripción de Azure donde creó el agente de consola, verá aparecer automáticamente un sistema de Azure Blob Storage en la página **Sistemas**. "Aprenda a administrar Azure Blob Storage desde la consola"

Paso 5: Proporcionar permisos al agente de la consola

Ahora que ha creado el agente de consola, debe proporcionarle los permisos que configuró previamente. Al proporcionar los permisos, se permite que el agente de la consola administre sus datos y la infraestructura de almacenamiento en Azure.

Rol personalizado

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.

¿Que sigue?

Ir a la "NetApp Console" para comenzar a utilizar el agente de consola.

Director de servicio

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 consola ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Instalar manualmente el agente de consola en Azure

Para instalar manualmente el agente de consola en su propio host Linux, debe revisar los requisitos del host, configurar su red, preparar los permisos de Azure, instalar el agente de consola y luego proporcionar los permisos que preparó.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .
- Deberías revisarlo"Limitaciones del agente de consola" .

Paso 1: Revisar los requisitos del host

El software del agente de consola debe ejecutarse en un host que cumpla con los requisitos específicos del sistema operativo, requisitos de RAM, requisitos de puerto, etc.

> El agente de consola reserva el rango de UID y GID de 19000 a 19200. Este rango es fijo y no se puede modificar. Si algún software de terceros en su host utiliza UID o GID dentro de este rango, la instalación del agente fallará. NetApp recomienda utilizar un host que esté libre de software de terceros para evitar conflictos.

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.

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.

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 2: Instalar 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 2. 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 3: Configurar la red

Asegúrese de que la ubicación de red donde planea instalar el agente de consola admita los siguientes requisitos. Cumplir estos requisitos permite que el agente de la consola administre recursos y procesos dentro de su entorno de nube híbrida.

Región de Azure

Si usa Cloud Volumes ONTAP, el agente de la consola debe implementarse en la misma región de Azure que los sistemas Cloud Volumes ONTAP que administra, o en la "Par de regiones de Azure" para los sistemas Cloud Volumes ONTAP . Este requisito 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"

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde computadoras al usar la NetApp Console basada en web

Las computadoras que acceden a la consola desde un navegador web deben tener la capacidad de comunicarse con varios puntos finales. Necesitará usar la consola para configurar el agente de la consola y para el uso diario de la consola.

"Preparar la red para la consola de NetApp" .

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
\ 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.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para administrar recursos en las regiones de Azure China.
\ 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.

Puntos finales	Objetivo
\ 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.

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"

Paso 4: Configurar los permisos de implementación del agente de consola

Debe proporcionar permisos de Azure al agente de consola mediante una de las siguientes opciones:

- Opción 1: Asignar un rol personalizado a la máquina virtual de Azure mediante una identidad administrada asignada por el sistema.
- Opción 2: proporcione al agente de consola las credenciales de una entidad de servicio de Azure que tenga los permisos necesarios.

Siga los pasos para preparar los permisos para el agente de la consola.

Crear un rol personalizado para la implementación 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.

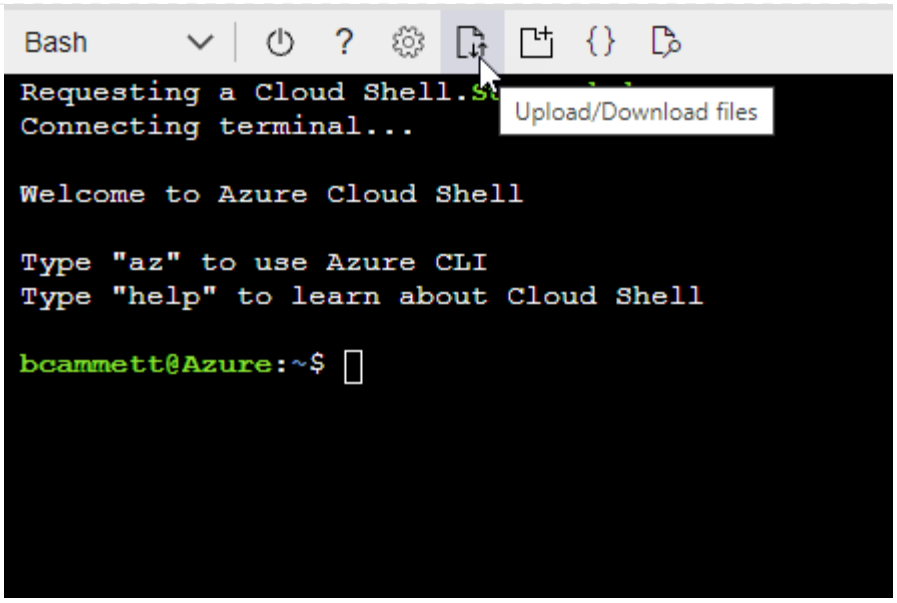
   Ejemplo

   ```
   "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
```

Director de servicio

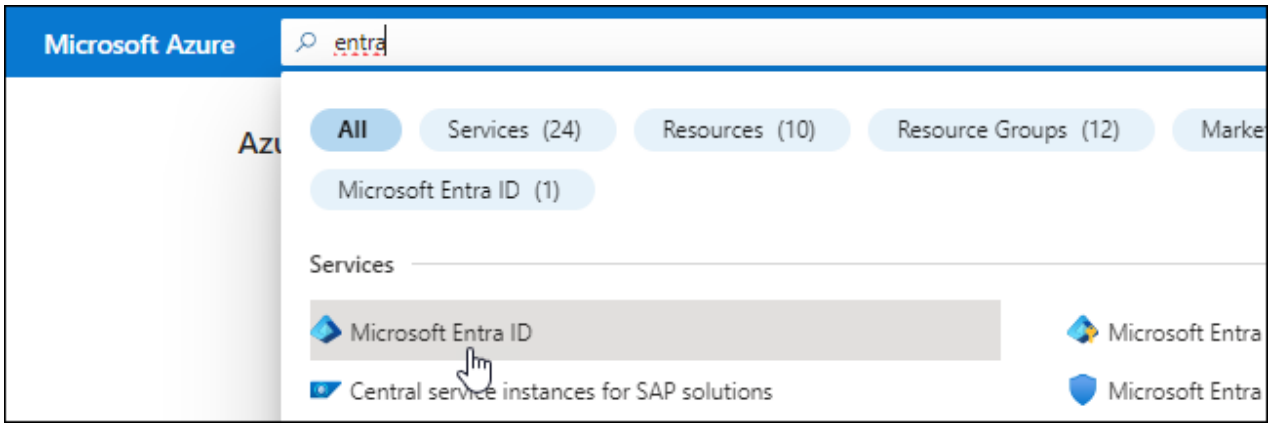
Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita el agente de consola.

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 .

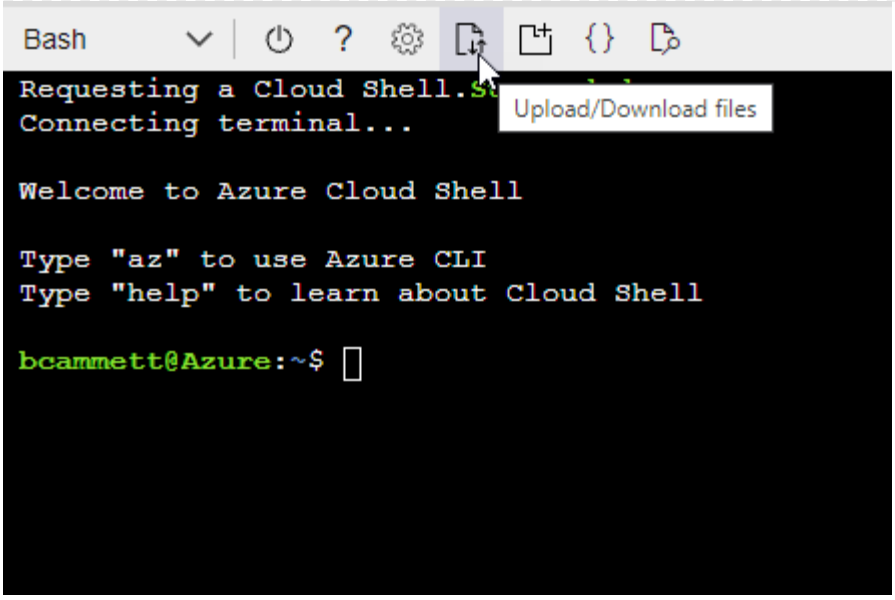
      Ejemplo

      ```
      "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**.

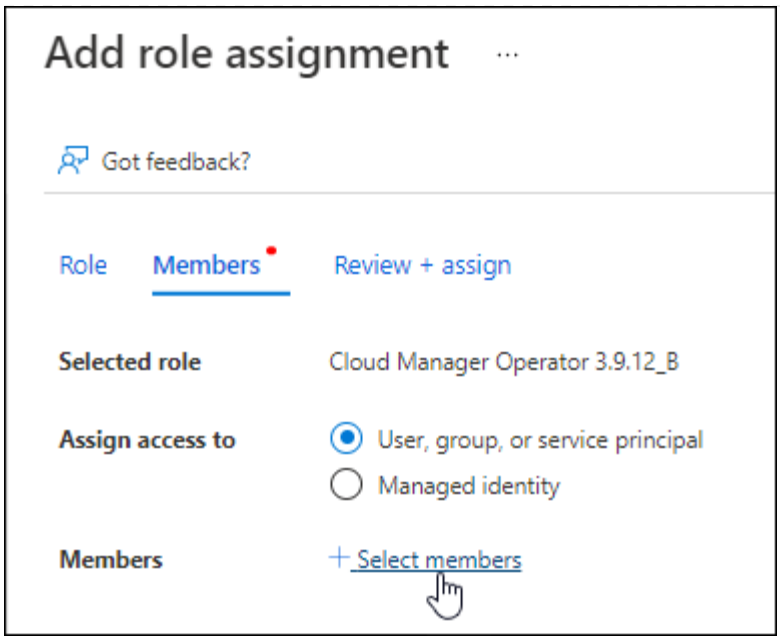
   b. Seleccione la suscripción.

   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**.

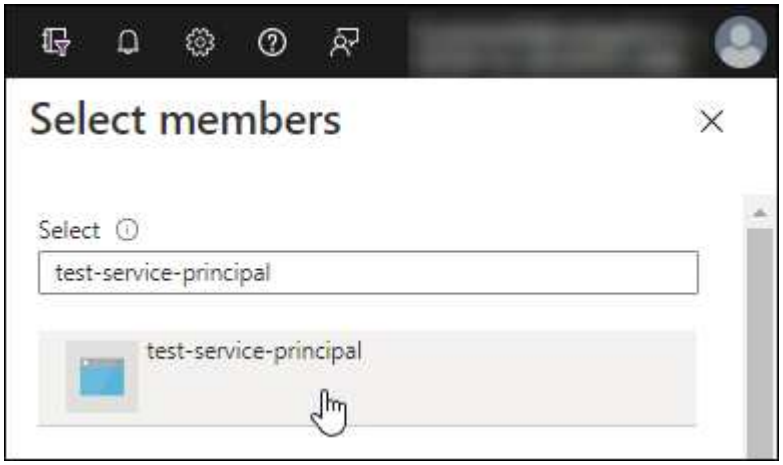
   e. En la pestaña **Miembros**, complete los siguientes pasos:

      - 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**.

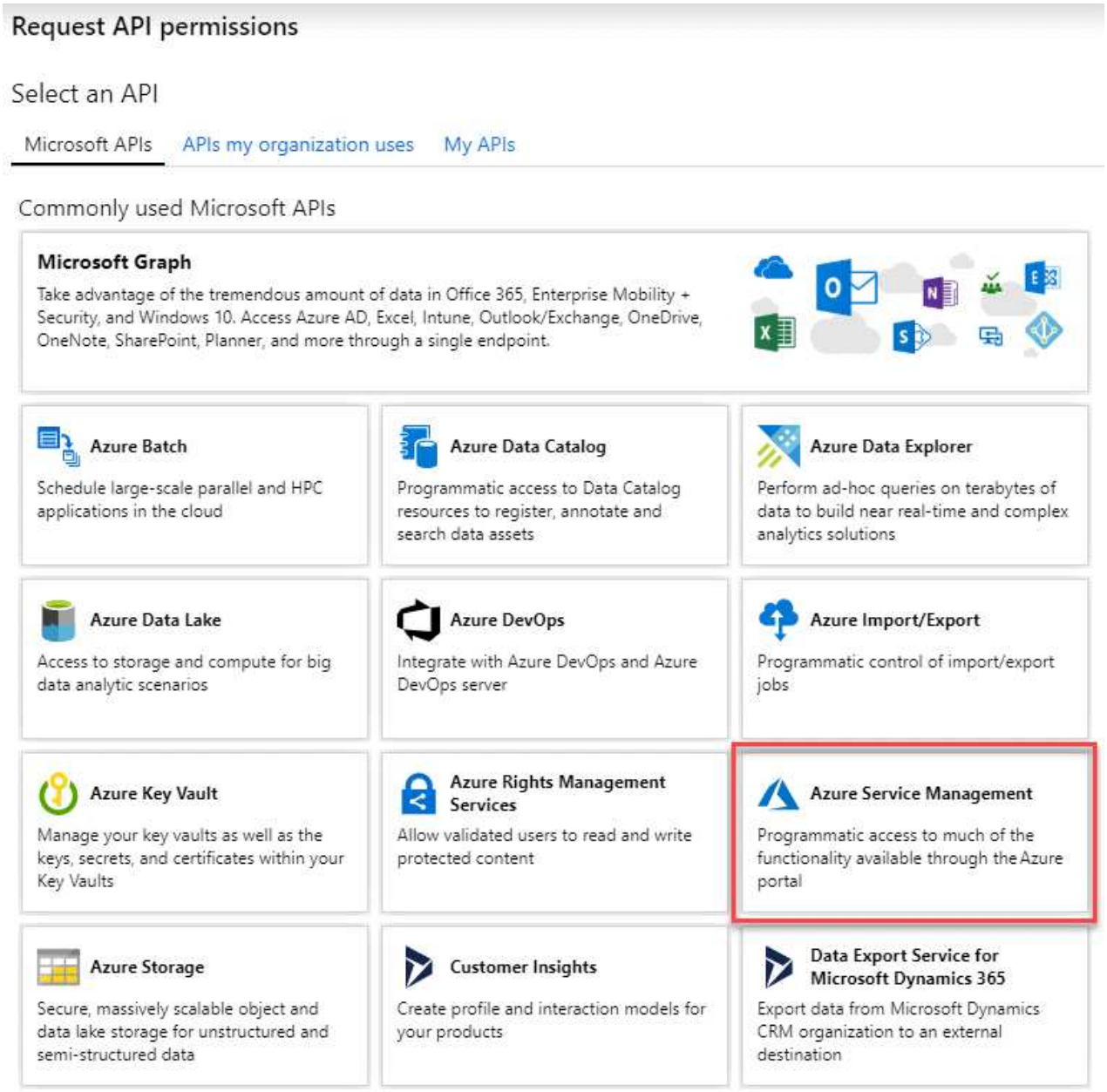
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

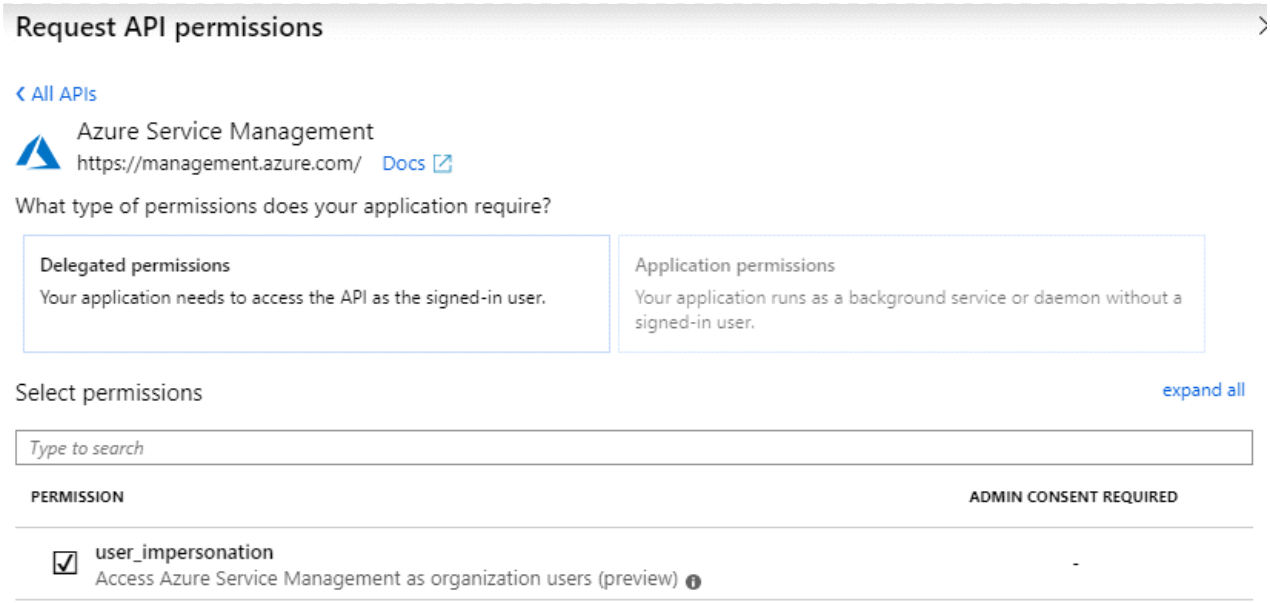
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

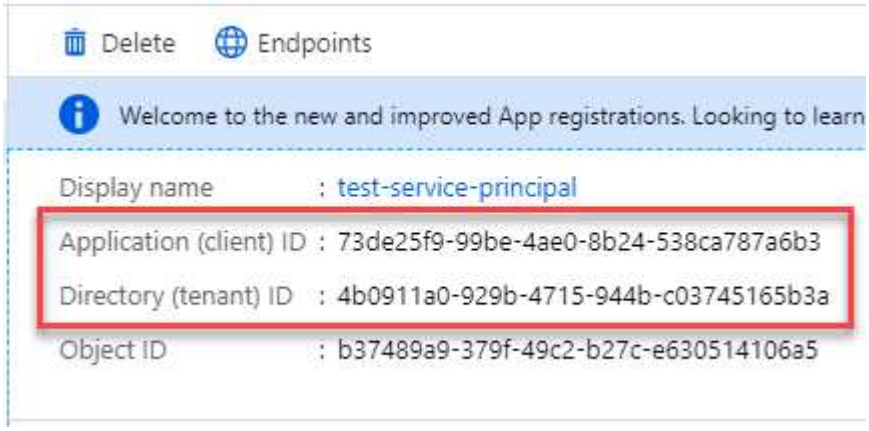


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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.

Paso 5: Instalar el agente de consola

Una vez completados los requisitos previos, puede instalar manualmente el software en su propio host Linux.

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".

- Una identidad administrada habilitada en la máquina virtual en Azure para que pueda 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"

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.

2. Espere a que se complete la instalación.

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

   Si la instalación falla, puede ver el informe de instalación y los registros para ayudarlo a solucionar los problemas."Aprenda a solucionar problemas de instalación."

1. Abra un navegador web desde un host que tenga una conexión a la máquina virtual del agente de consola e ingrese la siguiente URL:

   https://ipaddress

2. Después de iniciar sesión, configure el agente de la consola:
    a. Especifique la organización que se asociará con el agente de la consola.
    b. Introduzca un nombre para el sistema.
    c. En **¿Está ejecutando en un entorno seguro?** mantenga el modo restringido deshabilitado.

        Debes mantener el modo restringido deshabilitado porque estos pasos describen cómo usar la consola en modo estándar. Debe habilitar el modo restringido solo si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de backend. Si ese es el caso,"Siga los pasos para comenzar a utilizar la NetApp Console en modo restringido" .

    d. Seleccione **Comencemos**.

Si tiene Azure Blob Storage en la misma suscripción de Azure donde creó el agente de consola, verá aparecer automáticamente un sistema de Azure Blob Storage en la página **Sistemas**. "Aprenda a administrar Azure Blob Storage desde la NetApp Console"

Paso 6: Proporcionar permisos a la NetApp Console

Ahora que ha instalado el agente de consola, debe proporcionarle los permisos de Azure que configuró anteriormente. Al proporcionar los permisos, se permite que la consola administre sus datos y la infraestructura de almacenamiento en Azure.

Rol personalizado

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.

¿Que sigue?

Ir a la "NetApp Console" para comenzar a utilizar el agente de consola.

Director de servicio

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

El agente de consola ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre.

Google Cloud

Opciones de instalación del agente de consola en Google Cloud

Hay algunas formas diferentes de crear un agente de consola en Google Cloud. La forma más común es hacerlo directamente desde la NetApp Console .

Están disponibles las siguientes opciones de instalación:

- "Cree el agente de la consola directamente desde la consola"(esta es la opción estándar)

  Esta acción inicia una instancia de VM que ejecuta Linux y el software del agente de consola en una VPC de su elección.

- "Crear el agente de consola mediante Google Platform"

  Esta acción también inicia una instancia de VM que ejecuta Linux y el software del agente de la consola, pero la implementación se inicia directamente desde Google Cloud, en lugar de desde la consola.

- "Descargue e instale manualmente el software en su propio host Linux"

La opción de instalación que elija afectará su forma de prepararse para la instalación. Esto incluye cómo proporcionar a la consola los permisos necesarios para autenticar y administrar recursos en Google Cloud.

Crear un agente de consola en Google Cloud desde la NetApp Console

Puedes crear un agente de consola en Google Cloud desde la consola. Debe configurar su red, preparar los permisos de Google Cloud, habilitar las API de Google Cloud y luego crear el agente de consola.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .
- Deberías revisarlo"Limitaciones del agente de consola" .

Paso 1: Configurar la red

Configure la red para garantizar que el agente de la consola pueda administrar recursos, con conexiones a redes de destino y acceso a Internet saliente.

VPC y subred

Cuando crea el agente de consola, debe especificar la VPC y la subred donde debe residir.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de

almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
\ 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.
\ 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.

Puntos finales contactados desde la consola de NetApp

A medida que utiliza la NetApp Console basada en web que se proporciona a través de la capa SaaS, esta se comunica con varios puntos finales para completar tareas de administración de datos. Esto incluye los puntos finales que se contactan para implementar el agente de la consola desde la consola.

"Ver la lista de puntos finales contactados desde la consola de NetApp" .

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"

Implemente este requisito de red después de crear el agente de consola.

Paso 2: Configurar permisos para crear el agente de consola

Antes de poder implementar un agente de consola desde la consola, debe configurar permisos para el usuario de Google Platform que implementa la máquina virtual del agente de consola.

Pasos

1. Crear un rol personalizado en Google Platform:

   a. Cree un archivo YAML que incluya los siguientes permisos:

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
```

```
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
```

```
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Desde Google Cloud, activa Cloud Shell.

c. Sube el archivo YAML que incluye los permisos necesarios.

d. Cree un rol personalizado mediante el uso de `gcloud iam roles create` dominio.

El siguiente ejemplo crea un rol denominado "agentDeployment" a nivel de proyecto:

Roles de iam de gcloud crean un conector de implementación --proyecto=miproyecto --archivo=agent -deployment.yaml

"Documentación de Google Cloud: Creación y administración de roles personalizados"

2. Asigne este rol personalizado al usuario que implementará el agente de la consola desde la consola o mediante gcloud.

"Documentación de Google Cloud: Otorgar una función única"

Paso 3: Crea una cuenta de servicio de Google Cloud para usar con el agente

Se requiere una cuenta de servicio de Google Cloud para proporcionar al agente de la consola los permisos que necesita para administrar recursos en Google Cloud. Cuando cree el agente de consola, deberá asociar esta cuenta de servicio con la máquina virtual del agente de consola.

Es su responsabilidad actualizar la función personalizada a medida que se agreguen nuevos permisos en versiones posteriores. Si se requieren nuevos permisos, se enumerarán en las notas de la versión.

Pasos

1. Crear un rol personalizado en Google Cloud:

a. Cree un archivo YAML que incluya el contenido de"Permisos de cuenta de servicio para el agente de consola" .

b. Desde Google Cloud, activa Cloud Shell.

c. Sube el archivo YAML que incluye los permisos necesarios.

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 connector --project=myproject --file=agent.yaml
   ```

"Documentación de Google Cloud: Creación y administración de roles personalizados"

2. Cree una cuenta de servicio en Google Cloud y asígnele el rol:
   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"

3. Si planea implementar sistemas Cloud Volumes ONTAP en proyectos diferentes al proyecto donde reside el agente de la consola, deberá proporcionar a la cuenta de servicio del agente de la consola acceso a esos proyectos.

   Por ejemplo, supongamos que el agente de consola está en el proyecto 1 y desea crear sistemas Cloud Volumes ONTAP en el proyecto 2. Necesitará otorgar acceso a la cuenta de servicio en el proyecto 2.

   a. Desde el servicio IAM y administración, seleccione el proyecto de Google Cloud donde desea crear sistemas Cloud Volumes ONTAP .
   b. En la página **IAM**, seleccione **Otorgar acceso** y proporcione los detalles requeridos.
      - Ingrese el correo electrónico de la cuenta de servicio del agente de la consola.
      - Seleccione el rol personalizado del agente de consola.
      - Seleccione **Guardar**.

   Para más detalles, consulte "Documentación de Google Cloud"

Paso 4: Configurar permisos de VPC compartidos

Si está utilizando una VPC compartida para implementar recursos en un proyecto de servicio, deberá preparar sus permisos.

Esta tabla es de referencia y su entorno debe reflejar la tabla de permisos cuando se complete la configuración de IAM.

Ver permisos de VPC compartidos

Identidad	Creador	Alojado en	Permisos del proyecto de servicio	Permisos del proyecto anfitrión	Objetivo
Cuenta de Google para implementar el agente	Costumbre	Proyecto de servicio	"Política de implementación del agente"	computar.usuariodered	Implementación del agente en el proyecto de servicio
cuenta de servicio del agente	Costumbre	Proyecto de servicio	"Política de cuenta de servicio del agente"	Compute.NetworkUser administrador de implementación.editor	Implementación y mantenimiento de Cloud Volumes ONTAP y los servicios en el proyecto de servicio
Cuenta de servicio de Cloud Volumes ONTAP	Costumbre	Proyecto de servicio	Miembro de storage.admin: cuenta de servicio de la NetApp Console como serviceAccount.user	N/A	(Opcional) Para NetApp Cloud Tiering y NetApp Backup and Recovery
Agente de servicio de las API de Google	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	computar.usuariodered	Interactúa con las API de Google Cloud en nombre de la implementación. Permite que la consola utilice la red compartida.
Cuenta de servicio predeterminada de Google Compute Engine	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	computar.usuariodered	Implementa instancias de Google Cloud y la infraestructura computacional en nombre de la implementación. Permite que la consola utilice la red compartida.

Notas:

1. deploymentmanager.editor solo es necesario en el proyecto host si no pasa reglas de firewall a la implementación y elige dejar que la consola las cree por usted. La NetApp Console crea una implementación en el proyecto de host que contiene la regla de firewall VPC0 si no se especifica ninguna regla.
2. firewall.create y firewall.delete solo son necesarios si no pasa reglas de firewall a la implementación y elige dejar que la Consola las cree por usted. Estos permisos residen en el archivo .yaml de la cuenta de la consola. Si está implementando un par HA mediante una VPC compartida, estos permisos se

utilizarán para crear las reglas de firewall para VPC1, 2 y 3. Para todas las demás implementaciones, estos permisos también se utilizarán para crear reglas para VPC0.

3. Para la organización en niveles de nube, la cuenta de servicio de organización en niveles debe tener el rol serviceAccount.user en la cuenta de servicio, no solo en el nivel de proyecto. Actualmente, si asigna serviceAccount.user en el nivel del proyecto, los permisos no se muestran cuando consulta la cuenta de servicio con getIAMPolicy.

Paso 5: Habilitar las API de Google Cloud

Debe habilitar varias API de Google Cloud antes de implementar el agente de consola y Cloud Volumes ONTAP.

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))

"Documentación de Google Cloud: Habilitación de API"

Paso 6: Crear el agente de consola

Cree un agente de consola directamente desde la consola.

Al crear el agente de consola, se implementa una instancia de máquina virtual en Google Cloud utilizando una configuración predeterminada. No cambie a una instancia de VM más pequeña con menos CPU o menos RAM después de crear el agente de consola. "Obtenga información sobre la configuración predeterminada para el agente de la consola" .

Cuando implementa un agente en Google Cloud, el agente crea un depósito para almacenar archivos de implementación.

Antes de empezar

Debes tener lo siguiente:

- Los permisos de Google Cloud necesarios para crear el agente de consola y una cuenta de servicio para la máquina virtual del agente de consola.
- Una VPC y una subred que cumple con los requisitos de red.
- Detalles sobre un servidor proxy, si se requiere un proxy para el acceso a Internet desde el agente de la consola.

Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione **Implementar agente > Google Cloud**
3. En la página **Implementación de un agente**, revise los detalles sobre lo que necesitará. Tienes dos opciones:
   a. Seleccione **Continuar** para prepararse para la implementación utilizando la guía del producto. Cada paso de la guía del producto incluye la información contenida en esta página de la documentación.
   b. Seleccione **Ir a implementación** si ya se preparó siguiendo los pasos de esta página.
4. Siga los pasos del asistente para crear el agente de consola:
   - Si se le solicita, inicie sesión en su cuenta de Google, que debería tener los permisos necesarios para crear la instancia de máquina virtual.

     El formulario es propiedad de Google y está alojado por esta empresa. Sus credenciales no se proporcionan a NetApp.

   - **Detalles**: Ingrese un nombre para la instancia de la máquina virtual, especifique las etiquetas, seleccione un proyecto y luego seleccione la cuenta de servicio que tenga los permisos necesarios (consulte la sección anterior para obtener más detalles).
   - **Ubicación**: especifique una región, zona, VPC y subred para la instancia.
   - **Red**: elija si desea habilitar una dirección IP pública y, opcionalmente, especificar una configuración de proxy.
   - **Etiquetas de red**: agregue una etiqueta de red a la instancia del agente de consola si usa un proxy transparente. Las etiquetas de red deben comenzar con una letra minúscula y pueden contener letras minúsculas, números y guiones. Las etiquetas deben terminar con una letra minúscula o un número. Por ejemplo, puede utilizar la etiqueta "console-agent-proxy".
   - **Política de firewall**: elija si desea crear una nueva política de firewall o si desea seleccionar una política de firewall existente que permita las reglas de entrada y salida requeridas.

     "Reglas de firewall en Google Cloud"
5. Revise sus selecciones para verificar que su configuración sea correcta.
   a. La casilla de verificación **Validar configuración del agente** está marcada de forma predeterminada para que la consola valide los requisitos de conectividad de red cuando se implementa. Si la consola no logra implementar el agente, proporciona un informe para ayudarlo a solucionar el problema. Si la implementación se realiza correctamente, no se proporciona ningún informe.

   Si todavía estás usando el"puntos finales anteriores" utilizado para actualizaciones de agente, la validación falla con un error. Para evitar esto, desmarque la casilla de verificación para omitir la comprobación de validación.
6. Seleccione **Agregar**.

   El agente estará listo en aproximadamente 10 minutos; permanezca en la página hasta que se complete el proceso.

Resultado

Una vez completado el proceso, el agente de consola estará disponible para su uso.

Si la implementación falla, puedes descargar un informe y registros desde la Consola para ayudarte a solucionar los problemas."Aprenda a solucionar problemas de instalación."

Si tiene depósitos de Google Cloud Storage en la misma cuenta de Google Cloud donde creó el agente de consola, verá aparecer automáticamente un sistema de Google Cloud Storage en la página **Sistemas**. "Aprenda a administrar Google Cloud Storage desde la consola"

Crear un agente de consola desde Google Cloud

Para crear un agente de consola en Google Cloud mediante Google Cloud, debe configurar su red, preparar los permisos de Google Cloud, habilitar las API de Google Cloud y, luego, crear el agente de consola.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .
- Deberías revisarlo"Limitaciones del agente de consola" .

Paso 1: Configurar la red

Configure la red para permitir que el agente de la consola administre recursos y se conecte a redes de destino e Internet.

VPC y subred

Cuando crea el agente de consola, debe especificar la VPC y la subred donde debe residir.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
\ 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	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.

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.

Puntos finales contactados desde la consola de NetApp

A medida que utiliza la NetApp Console basada en web que se proporciona a través de la capa SaaS, esta se comunica con varios puntos finales para completar tareas de administración de datos. Esto incluye los puntos finales que se contactan para implementar el agente de la consola desde la consola.

"Ver la lista de puntos finales contactados desde la consola de NetApp" .

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"

Implemente este requisito de red después de crear el agente de consola.

Paso 2: Configurar permisos para crear el agente de consola

Configure permisos para que el usuario de Google Cloud implemente la máquina virtual del agente de consola desde Google Cloud.

Pasos

1. Crear un rol personalizado en Google Platform:

   a. Cree un archivo YAML que incluya los siguientes permisos:

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Desde Google Cloud, activa Cloud Shell.

c. Sube el archivo YAML que incluye los permisos necesarios.

d. Cree un rol personalizado mediante el uso de `gcloud iam roles create` dominio.

El siguiente ejemplo crea un rol denominado "connectorDeployment" a nivel de proyecto:

Roles de iam de gcloud crean un conectorDeployment --project=myproject --file=connector -deployment.yaml

"Documentación de Google Cloud: Creación y administración de roles personalizados"

2. Asigne esta función personalizada al usuario que implementa el agente de consola desde Google Cloud.

"Documentación de Google Cloud: Otorgar una función única"

Paso 3: Configurar permisos para las operaciones del agente de la consola

Se requiere una cuenta de servicio de Google Cloud para proporcionar al agente de la consola los permisos que necesita para administrar recursos en Google Cloud. Cuando cree el agente de consola, deberá asociar esta cuenta de servicio con la máquina virtual del agente de consola.

Es su responsabilidad actualizar la función personalizada a medida que se agreguen nuevos permisos en versiones posteriores. Si se requieren nuevos permisos, se enumerarán en las notas de la versión.

Pasos

1. Crear un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya el contenido de"Permisos de cuenta de servicio para el agente de consola" .

   b. Desde Google Cloud, activa Cloud Shell.

   c. Sube el archivo YAML que incluye los permisos necesarios.

   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 connector --project=myproject --file=agent.yaml
      ```

   "Documentación de Google Cloud: Creación y administración de roles personalizados"

2. Cree una cuenta de servicio en Google Cloud y asígnele el rol:

   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"

3. Si planea implementar sistemas Cloud Volumes ONTAP en proyectos diferentes al proyecto donde reside el agente de la consola, deberá proporcionar a la cuenta de servicio del agente de la consola acceso a esos proyectos.

   Por ejemplo, supongamos que el agente de consola está en el proyecto 1 y desea crear sistemas Cloud Volumes ONTAP en el proyecto 2. Necesitará otorgar acceso a la cuenta de servicio en el proyecto 2.

   a. Desde el servicio IAM y administración, seleccione el proyecto de Google Cloud donde desea crear sistemas Cloud Volumes ONTAP .

b. En la página **IAM**, seleccione **Otorgar acceso** y proporcione los detalles requeridos.
   - Ingrese el correo electrónico de la cuenta de servicio del agente de la consola.
   - Seleccione el rol personalizado del agente de consola.
   - Seleccione **Guardar**.

Para más detalles, consulte "Documentación de Google Cloud"

Paso 4: Configurar permisos de VPC compartidos

Si está utilizando una VPC compartida para implementar recursos en un proyecto de servicio, deberá preparar sus permisos.

Esta tabla es de referencia y su entorno debe reflejar la tabla de permisos cuando se complete la configuración de IAM.

Ver permisos de VPC compartidos

Identidad	Creador	Alojado en	Permisos del proyecto de servicio	Permisos del proyecto anfitrión	Objetivo
Cuenta de Google para implementar el agente	Costumbre	Proyecto de servicio	"Política de implementación del agente"	computar.usuariodered	Implementación del agente en el proyecto de servicio
cuenta de servicio del agente	Costumbre	Proyecto de servicio	"Política de cuenta de servicio del agente"	Compute.NetworkUser administrador de implementación.editor	Implementación y mantenimiento de Cloud Volumes ONTAP y los servicios en el proyecto de servicio
Cuenta de servicio de Cloud Volumes ONTAP	Costumbre	Proyecto de servicio	Miembro de storage.admin: cuenta de servicio de la NetApp Console como serviceAccount.user	N/A	(Opcional) Para NetApp Cloud Tiering y NetApp Backup and Recovery
Agente de servicio de las API de Google	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	computar.usuariodered	Interactúa con las API de Google Cloud en nombre de la implementación. Permite que la consola utilice la red compartida.
Cuenta de servicio predeterminada de Google Compute Engine	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	computar.usuariodered	Implementa instancias de Google Cloud y la infraestructura computacional en nombre de la implementación. Permite que la consola utilice la red compartida.

Notas:

1. deploymentmanager.editor solo es necesario en el proyecto host si no pasa reglas de firewall a la implementación y elige dejar que la consola las cree por usted. La NetApp Console crea una implementación en el proyecto de host que contiene la regla de firewall VPC0 si no se especifica ninguna regla.
2. firewall.create y firewall.delete solo son necesarios si no pasa reglas de firewall a la implementación y elige dejar que la Consola las cree por usted. Estos permisos residen en el archivo .yaml de la cuenta de la consola. Si está implementando un par HA mediante una VPC compartida, estos permisos se

utilizarán para crear las reglas de firewall para VPC1, 2 y 3. Para todas las demás implementaciones, estos permisos también se utilizarán para crear reglas para VPC0.

3. Para la organización en niveles de nube, la cuenta de servicio de organización en niveles debe tener el rol serviceAccount.user en la cuenta de servicio, no solo en el nivel de proyecto. Actualmente, si asigna serviceAccount.user en el nivel del proyecto, los permisos no se muestran cuando consulta la cuenta de servicio con getIAMPolicy.

Paso 5: Habilitar las API de Google Cloud

Habilite varias API de Google Cloud antes de implementar el agente de consola y Cloud Volumes ONTAP.

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))

"Documentación de Google Cloud: Habilitación de API"

Paso 6: Crear el agente de consola

Cree un agente de consola mediante Google Cloud.

Al crear el agente de consola, se implementa una instancia de VM en Google Cloud con la configuración predeterminada. No cambie a una instancia de VM más pequeña con menos CPU o menos RAM después de crear el agente de consola. "Obtenga información sobre la configuración predeterminada para el agente de la consola" .

Antes de empezar

Debes tener lo siguiente:

- Los permisos de Google Cloud necesarios para crear el agente de consola y una cuenta de servicio para la máquina virtual del agente de consola.
- Una VPC y una subred que cumple con los requisitos de red.
- Una comprensión de los requisitos de la instancia de VM.
  - **CPU**: 8 núcleos u 8 vCPU
  - **RAM**: 32 GB
  - **Tipo de máquina**: Recomendamos n2-standard-8.

    El agente de consola es compatible con Google Cloud en una instancia de VM con un sistema

operativo que admite funciones de VM protegida.

Pasos

1. Inicie sesión en el SDK de Google Cloud utilizando su método preferido.

   Este ejemplo utiliza un shell local con el SDK de gcloud instalado, pero también puedes usar Google Cloud Shell.

   Para obtener más información sobre el SDK de Google Cloud, visite el sitio web"Página de documentación del SDK de Google Cloud" .

2. Verifique que haya iniciado sesión como un usuario que tiene los permisos necesarios definidos en la sección anterior:

   ```
   gcloud auth list
   ```

   El resultado debe mostrar lo siguiente, donde la cuenta de usuario * es la cuenta de usuario con la que se desea iniciar sesión:

   ```
   Credentialed Accounts
   ACTIVE  ACCOUNT
        some_user_account@domain.com
   *    desired_user_account@domain.com
   To set the active account, run:
    $ gcloud config set account `ACCOUNT`
   Updates are available for some Cloud SDK components. To install them,
   please run:
   $ gcloud components update
   ```

3. Ejecutar el `gcloud compute instances create` dominio:

   ```
   gcloud compute instances create <instance-name>
     --machine-type=n2-standard-8
     --image-project=netapp-cloudmanager
     --image-family=cloudmanager
     --scopes=cloud-platform
     --project=<project>
     --service-account=<service-account>
     --zone=<zone>
     --no-address
     --tags <network-tag>
     --network <network-path>
     --subnet <subnet-path>
     --boot-disk-kms-key <kms-key-path>
   ```

nombre de instancia
El nombre de instancia deseado para la instancia de VM.

proyecto
(Opcional) El proyecto donde desea implementar la VM.

cuenta de servicio
La cuenta de servicio especificada en la salida del paso 2.

zona
La zona donde desea implementar la máquina virtual

sin dirección
(Opcional) No se utiliza ninguna dirección IP externa (necesita un NAT en la nube o un proxy para enrutar el tráfico a Internet público)

etiqueta de red
(Opcional) Agregue etiquetado de red para vincular una regla de firewall mediante etiquetas a la instancia del agente de la consola

ruta de red
(Opcional) Agregue el nombre de la red donde se implementará el agente de consola (para una VPC compartida, necesita la ruta completa)

ruta de subred
(Opcional) Agregue el nombre de la subred donde se implementará el agente de consola (para una VPC compartida, necesita la ruta completa)

ruta de la clave kms
(Opcional) Agregue una clave KMS para cifrar los discos del agente de la consola (también se deben aplicar los permisos de IAM)

Para obtener más información sobre estas banderas, visite el sitio"Documentación del SDK de Google Cloud Computing" .

Al ejecutar el comando se implementa el agente de consola. La instancia del agente de consola y el software deberían estar ejecutándose en aproximadamente cinco minutos.

4. Abra un navegador web e ingrese la URL del host del agente de la consola:

   La URL del host de la consola puede ser un host local, una dirección IP privada o una dirección IP pública, según la configuración del host. Por ejemplo, si el agente de la consola está en la nube pública sin una dirección IP pública, debe ingresar una dirección IP privada de un host que tenga una conexión al host del agente de la consola.

5. Después de iniciar sesión, configure el agente de la consola:
   a. Especifique la organización de la consola que se asociará con el agente de la consola.

      "Aprenda sobre la gestión de identidad y acceso" .

   b. Introduzca un nombre para el sistema.

Resultado

El agente de consola ahora está instalado y configurado con su organización de consola.

Abra un navegador web y vaya a "NetApp Console" para comenzar a utilizar el agente de consola.

Instalar manualmente el agente de la consola en Google Cloud

Para instalar manualmente el agente de la consola en su propio host Linux, debe revisar los requisitos del host, configurar su red, preparar los permisos de Google Cloud, habilitar las API de Google Cloud, instalar la consola y luego proporcionar los permisos que preparó.

Antes de empezar

- Deberías tener una"comprensión de los agentes de consola" .
- Deberías revisarlo"Limitaciones del agente de consola" .

Paso 1: Revisar los requisitos del host

El software del agente de consola debe ejecutarse en un host que cumpla con los requisitos específicos del sistema operativo, requisitos de RAM, requisitos de puerto, etc.

> El agente de consola reserva el rango de UID y GID de 19000 a 19200. Este rango es fijo y no se puede modificar. Si algún software de terceros en su host utiliza UID o GID dentro de este rango, la instalación del agente fallará. NetApp recomienda utilizar un host que esté libre de software de terceros para evitar conflictos.

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 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 .

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
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 .
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 .

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Compatible con modo de aplicación o modo permisivo	Ubuntu		24,04 LTS	3.9.45 o posterior con la NetApp Console en modo estándar o modo restringido
Motor Docker 23.06 a 28.0.0.	No compatible		22,04 LTS	3.9.50 o posterior

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"

Paso 2: Instalar 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 3. 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 3: Configurar la red

Configure su red para que el agente de la consola pueda administrar recursos y procesos dentro de su entorno de nube híbrida. Por ejemplo, debe asegurarse de que haya conexiones disponibles para las redes de destino y que el acceso a Internet saliente esté disponible.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde computadoras al usar la NetApp Console basada en web

Las computadoras que acceden a la consola desde un navegador web deben tener la capacidad de comunicarse con varios puntos finales. Necesitará usar la consola para configurar el agente de la consola y para el uso diario de la consola.

"Preparar la red para la consola de NetApp" .

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
\ 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.
\ 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.

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://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.

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"

Paso 4: Configurar permisos para el agente de la consola

Se requiere una cuenta de servicio de Google Cloud para proporcionar al agente de la consola los permisos que necesita para administrar recursos en Google Cloud. Cuando cree el agente de consola, deberá asociar esta cuenta de servicio con la máquina virtual del agente de consola.

Es su responsabilidad actualizar la función personalizada a medida que se agreguen nuevos permisos en versiones posteriores. Si se requieren nuevos permisos, se enumerarán en las notas de la versión.

Pasos

1. Crear un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya el contenido de"Permisos de cuenta de servicio para el agente de consola" .

   b. Desde Google Cloud, activa Cloud Shell.

   c. Sube el archivo YAML que incluye los permisos necesarios.

   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 connector --project=myproject --file=agent.yaml
      ```

   "Documentación de Google Cloud: Creación y administración de roles personalizados"

2. Cree una cuenta de servicio en Google Cloud y asígnele el rol:

   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"

3. Si planea implementar sistemas Cloud Volumes ONTAP en proyectos diferentes al proyecto donde reside el agente de la consola, deberá proporcionar a la cuenta de servicio del agente de la consola acceso a

esos proyectos.

Por ejemplo, supongamos que el agente de consola está en el proyecto 1 y desea crear sistemas Cloud Volumes ONTAP en el proyecto 2. Necesitará otorgar acceso a la cuenta de servicio en el proyecto 2.

a. Desde el servicio IAM y administración, seleccione el proyecto de Google Cloud donde desea crear sistemas Cloud Volumes ONTAP .
b. En la página **IAM**, seleccione **Otorgar acceso** y proporcione los detalles requeridos.
   - Ingrese el correo electrónico de la cuenta de servicio del agente de la consola.
   - Seleccione el rol personalizado del agente de consola.
   - Seleccione **Guardar**.

Para más detalles, consulte "Documentación de Google Cloud"

Paso 5: Configurar permisos de VPC compartidos

Si está utilizando una VPC compartida para implementar recursos en un proyecto de servicio, deberá preparar sus permisos.

Esta tabla es de referencia y su entorno debe reflejar la tabla de permisos cuando se complete la configuración de IAM.

Ver permisos de VPC compartidos

Identidad	Creador	Alojado en	Permisos del proyecto de servicio	Permisos del proyecto anfitrión	Objetivo
Cuenta de Google para implementar el agente	Costumbre	Proyecto de servicio	"Política de implementación del agente"	computar.usuariodered	Implementación del agente en el proyecto de servicio
cuenta de servicio del agente	Costumbre	Proyecto de servicio	"Política de cuenta de servicio del agente"	Compute.NetworkUser administrador de implementación.editor	Implementación y mantenimiento de Cloud Volumes ONTAP y los servicios en el proyecto de servicio
Cuenta de servicio de Cloud Volumes ONTAP	Costumbre	Proyecto de servicio	Miembro de storage.admin: cuenta de servicio de la NetApp Console como serviceAccount.user	N/A	(Opcional) Para NetApp Cloud Tiering y NetApp Backup and Recovery
Agente de servicio de las API de Google	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	computar.usuariodered	Interactúa con las API de Google Cloud en nombre de la implementación. Permite que la consola utilice la red compartida.
Cuenta de servicio predeterminada de Google Compute Engine	Google Cloud	Proyecto de servicio	(Predeterminado) Editor	computar.usuariodered	Implementa instancias de Google Cloud y la infraestructura computacional en nombre de la implementación. Permite que la consola utilice la red compartida.

Notas:

1. deploymentmanager.editor solo es necesario en el proyecto host si no pasa reglas de firewall a la implementación y elige dejar que la consola las cree por usted. La NetApp Console crea una implementación en el proyecto de host que contiene la regla de firewall VPC0 si no se especifica ninguna regla.
2. firewall.create y firewall.delete solo son necesarios si no pasa reglas de firewall a la implementación y elige dejar que la Consola las cree por usted. Estos permisos residen en el archivo .yaml de la cuenta de la consola. Si está implementando un par HA mediante una VPC compartida, estos permisos se

utilizarán para crear las reglas de firewall para VPC1, 2 y 3. Para todas las demás implementaciones, estos permisos también se utilizarán para crear reglas para VPC0.

3. Para la organización en niveles de nube, la cuenta de servicio de organización en niveles debe tener el rol serviceAccount.user en la cuenta de servicio, no solo en el nivel de proyecto. Actualmente, si asigna serviceAccount.user en el nivel del proyecto, los permisos no se muestran cuando consulta la cuenta de servicio con getIAMPolicy.

Paso 6: Habilitar las API de Google Cloud

Se deben habilitar varias API de Google Cloud antes de poder implementar un agente de consola 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))

"Documentación de Google Cloud: Habilitación de API"

Paso 7: Instalar el agente de consola

Una vez completados los requisitos previos, puede instalar manualmente el software en su propio host Linux.

Cuando implementa un agente, el sistema también crea un depósito de Google Cloud para almacenar archivos de implementación.

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".

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.

2. Espere a que se complete la instalación.

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

   Si la instalación falla, puede ver el informe de instalación y los registros para ayudarlo a solucionar los problemas."Aprenda a solucionar problemas de instalación."

1. Abra un navegador web desde un host que tenga una conexión a la máquina virtual del agente de consola e ingrese la siguiente URL:

   https://ipaddress

2. Después de iniciar sesión, configure el agente de la consola:

   a. Especifique la organización que se asociará con el agente de la consola.

   b. Introduzca un nombre para el sistema.

   c. En **¿Está ejecutando en un entorno seguro?** mantenga el modo restringido deshabilitado.

      Debes mantener el modo restringido deshabilitado porque estos pasos describen cómo usar la consola en modo estándar. Debe habilitar el modo restringido solo si tiene un entorno seguro y desea desconectar esta cuenta de los servicios de backend. Si ese es el caso,"Siga los pasos para comenzar a utilizar la NetApp Console en modo restringido" .

   d. Seleccione **Comencemos**.

   Si la instalación falla, puede ver registros y un informe para ayudarlo a solucionar problemas."Aprenda a solucionar problemas de instalación."

Si tiene depósitos de Google Cloud Storage en la misma cuenta de Google Cloud donde creó el agente de consola, verá aparecer automáticamente un sistema de Google Cloud Storage en la página **Sistemas**. "Aprenda a administrar Google Cloud Storage desde la NetApp Console"

Paso 8: Proporcionar permisos al agente de la consola

Debes proporcionar al agente de la consola los permisos de Google Cloud que configuraste previamente. Al proporcionar los permisos, se permite que el agente de la consola administre sus datos y la infraestructura de almacenamiento en Google Cloud.

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 de Google Cloud, otorgue acceso agregando la cuenta de servicio con el rol de agente de consola a ese proyecto. Necesitarás repetir este paso para cada proyecto.

Instalar un agente en las instalaciones

Instalar manualmente un agente de consola local

Instale un agente de consola local y luego inicie sesión y configúrelo para que funcione con su organización de consola.

Si es un usuario de VMWare, puede utilizar un OVA para instalar un agente de consola en su VCenter."Obtenga más información sobre cómo instalar un agente en un VCenter."

Antes de realizar la instalación, deberá asegurarse de que su host (VM o host Linux) cumpla con los requisitos y de que el agente de la consola tenga acceso saliente a Internet y a las redes específicas. Si planea utilizar servicios de datos de NetApp u opciones de almacenamiento en la nube como Cloud Volumes ONTAP, deberá crear credenciales en su proveedor de nube para agregarlas a la consola para que el agente de la consola pueda realizar acciones en la nube en su nombre.

Prepárese para instalar el agente de consola

Antes de instalar un agente de consola, debe asegurarse de tener un equipo host que cumpla con los requisitos de instalación. También deberá trabajar con su administrador de red para garantizar que el agente de la consola tenga acceso saliente a los puntos finales requeridos y conexiones a las redes específicas.

Revisar los requisitos del host del agente de la consola

Ejecute el agente de consola en un host x86 que cumpla con los requisitos de sistema operativo, RAM y puerto. Asegúrese de que su host cumpla con estos requisitos antes de instalar el agente de consola.

El agente de consola reserva el rango de UID y GID de 19000 a 19200. Este rango es fijo y no se puede modificar. Si algún software de terceros en su host utiliza UID o GID dentro de este rango, la instalación del agente fallará. NetApp recomienda utilizar un host que esté libre de software de terceros para evitar conflictos.

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.

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 .

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
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 .
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 .

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Compatible con modo de aplicación o modo permisivo	Ubuntu		24,04 LTS	3.9.45 o posterior con la NetApp Console en modo estándar o modo restringido
Motor Docker 23.06 a 28.0.0.	No compatible		22,04 LTS	3.9.50 o posterior

Configurar el acceso a la red para el agente de la consola

Configure el acceso a la red para garantizar que el agente de la consola pueda administrar recursos. Necesita conexiones a redes de destino y acceso a Internet saliente a puntos finales específicos.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde computadoras al usar la NetApp Console basada en web

Las computadoras que acceden a la consola desde un navegador web deben tener la capacidad de comunicarse con varios puntos finales. Necesitará usar la consola para configurar el agente de la consola y para el uso diario de la consola.

"Preparar la red para la consola de NetApp" .

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Un agente de consola instalado en sus instalaciones no puede administrar recursos en Google Cloud. Si desea administrar los recursos de Google Cloud, debe instalar un agente en Google Cloud.

AWS

Cuando el agente de consola está instalado localmente, necesita acceso de red a los siguientes puntos finales de AWS para administrar los sistemas NetApp (como Cloud Volumes ONTAP) implementados en AWS.

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
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 .
\ 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.

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://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.

Azur

Cuando el agente de consola está instalado localmente, necesita acceso de red a los siguientes puntos de conexión de Azure para administrar los sistemas NetApp (como Cloud Volumes ONTAP) implementados en Azure.

Puntos finales	Objetivo
\ 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.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
\ 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.

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"

Crear permisos de nube de agente de consola para AWS o Azure

Si desea utilizar los servicios de datos de NetApp en AWS o Azure con un agente de consola local, deberá configurar permisos en su proveedor de nube y luego agregar las credenciales al agente de consola después de instalarlo.

Debes instalar el agente de consola en Google Cloud para administrar cualquier recurso que resida allí.

AWS

Cuando el agente de la consola está instalado localmente, debe proporcionarle a la consola permisos de AWS agregando claves de acceso para un usuario de IAM que tenga los permisos necesarios.

Debe utilizar este método de autenticación si el agente de consola está instalado localmente. No puedes utilizar un rol IAM.

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 necesite 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.

Resultado

Ahora debería tener claves de acceso para un usuario de IAM que tenga los permisos necesarios. Después de instalar el agente de la consola, asocie estas credenciales con el agente de la consola desde la consola.

Azur

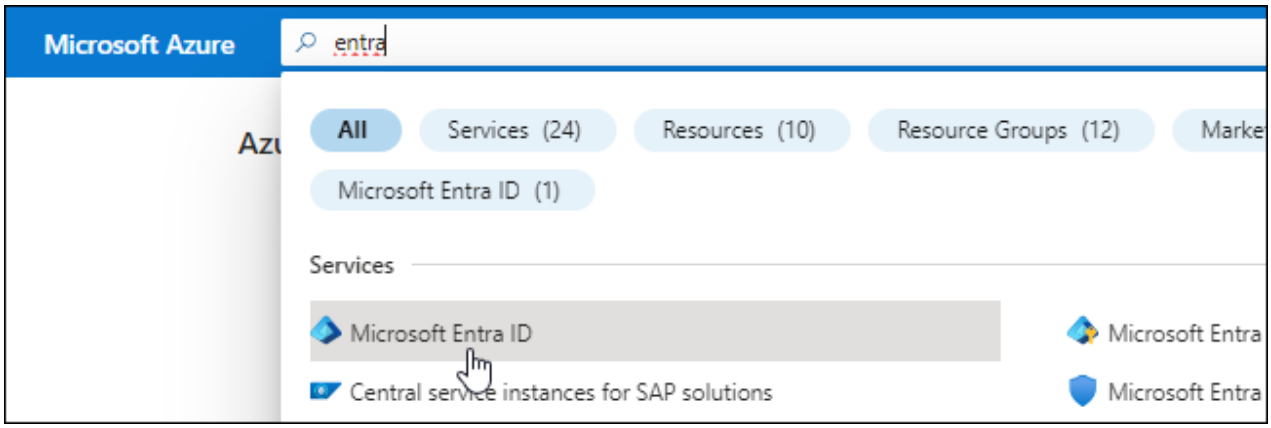
Cuando el agente de consola está instalado localmente, debe proporcionarle permisos de Azure configurando una entidad de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que necesita el agente de consola.

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 .

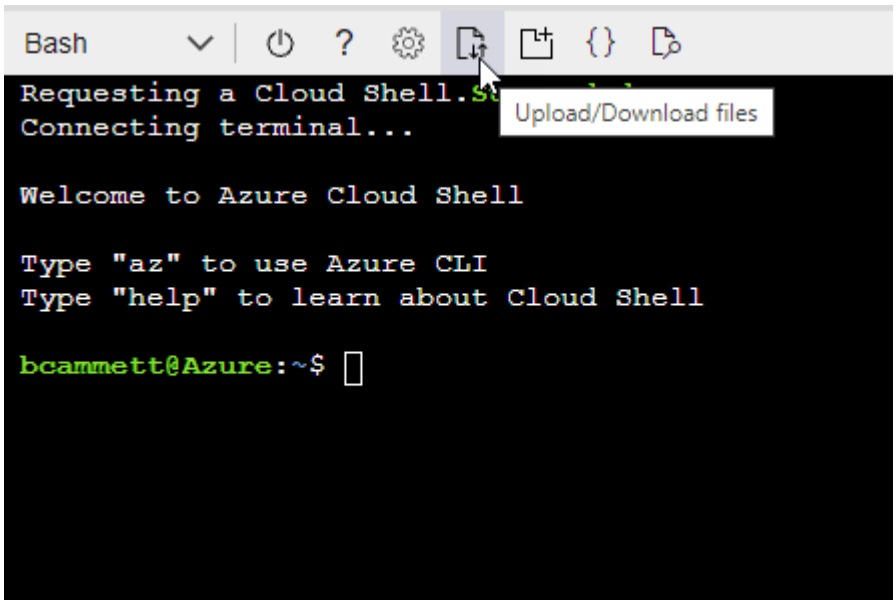
      Ejemplo

      ```
      "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:

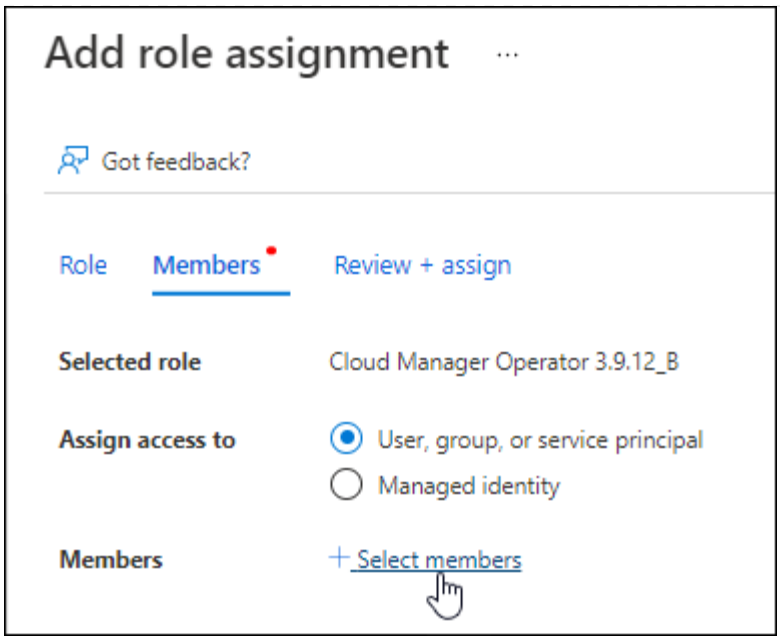
```
az role definition create --role-definition agent_Policy.json
```

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:

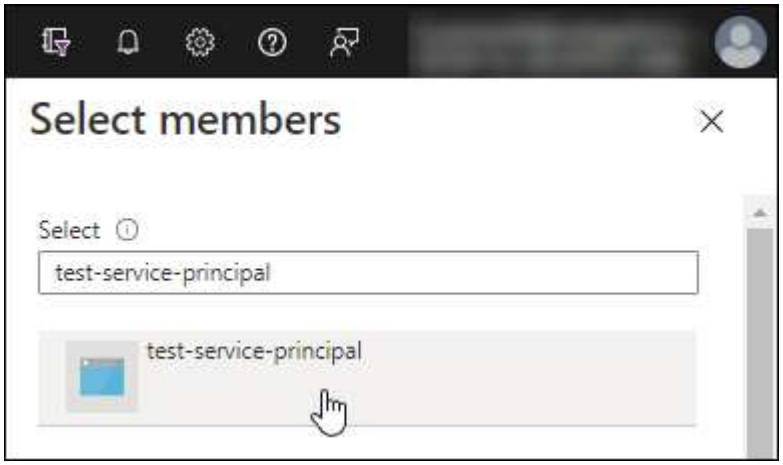
   a. Desde el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de rol**.
   d. En la pestaña **Rol**, seleccione el rol **Operador de consola** y seleccione **Siguiente**.
   e. En la pestaña **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**.

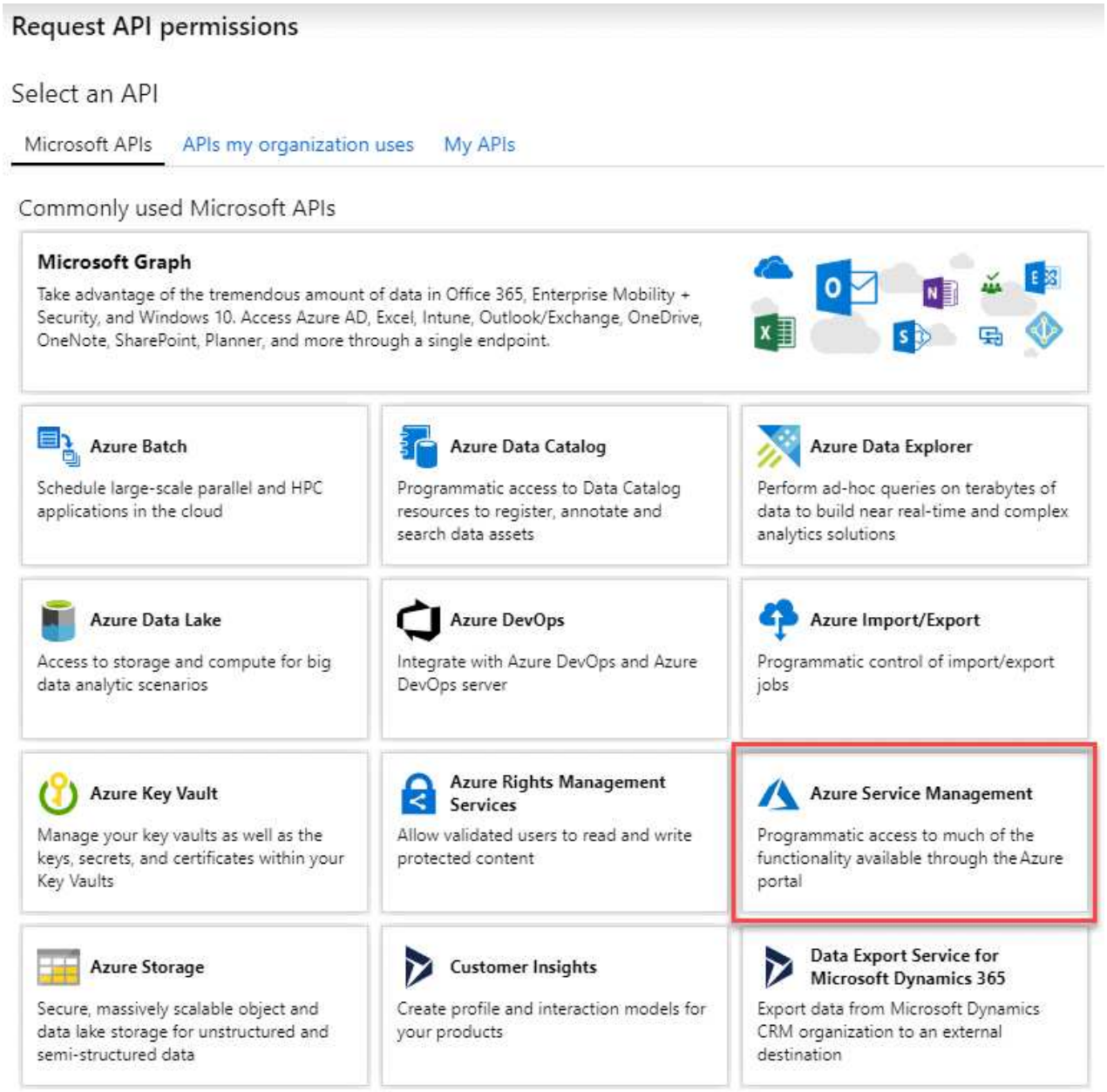
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

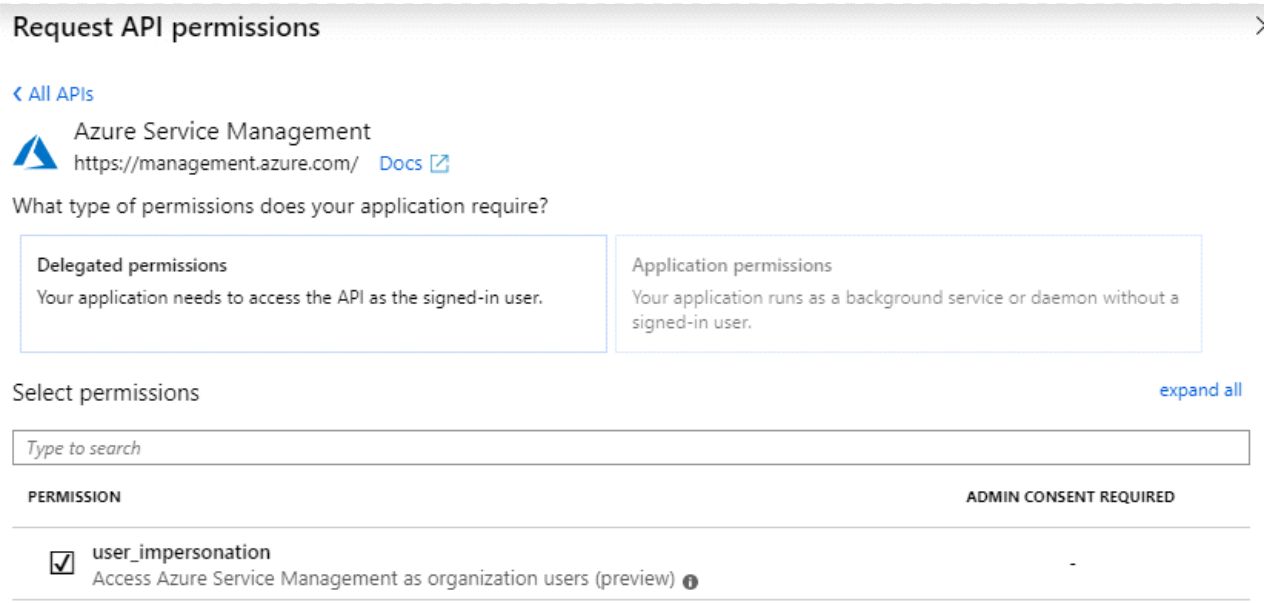
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

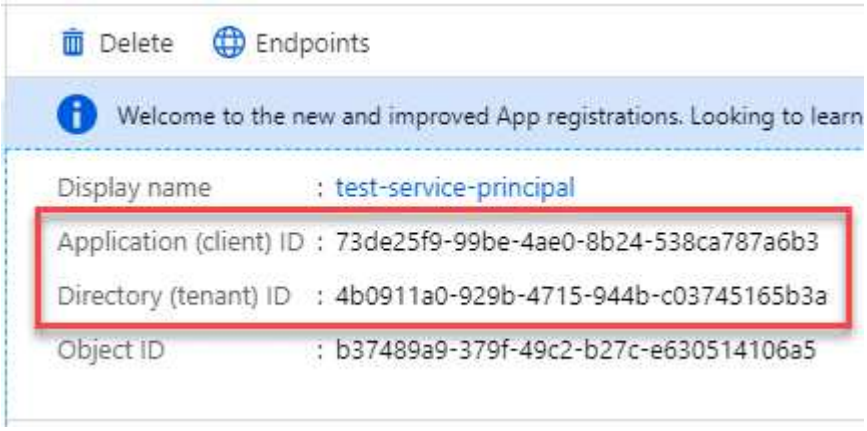


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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

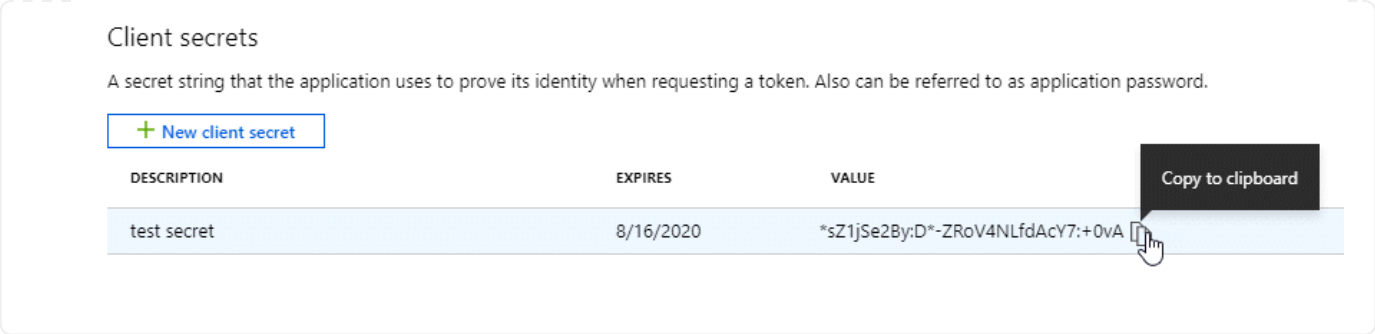
1. En el servicio **Microsoft Entra ID**, seleccione **Registros de aplicaciones** y seleccione la aplicación.
2. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)**.



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.



Instalar manualmente un agente de consola

Cuando instala manualmente un agente de consola, debe preparar el entorno de su máquina para que cumpla con los requisitos. Necesitarás una máquina Linux y necesitarás instalar Podman o Docker, dependiendo de tu sistema operativo Linux.

Instalar 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 4. 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
```

Instalar el agente de consola manualmente

Descargue e instale el software del agente de consola en un host Linux existente en las instalaciones.

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".

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.

¿Que sigue?

Necesitará registrar el agente de consola dentro de la NetApp Console.

Registrar el agente de consola con NetApp Console

Inicie sesión en la consola y asocie el agente de la consola con su organización. La forma de iniciar sesión depende del modo en que esté utilizando la Consola. Si está utilizando la consola en modo estándar, inicie sesión a través del sitio web de SaaS. Si está utilizando la consola en modo restringido, inicie sesión localmente desde el host del agente de la consola.

Pasos

1. Abra un navegador web e ingrese la URL del host del agente de la consola:

   La URL del host de la consola puede ser un host local, una dirección IP privada o una dirección IP pública, según la configuración del host. Por ejemplo, si el agente de la consola está en la nube pública sin una dirección IP pública, debe ingresar una dirección IP privada de un host que tenga una conexión al host del agente de la consola.

2. Regístrate o inicia sesión.
3. Después de iniciar sesión, configure la consola:
   a. Especifique la organización de la consola que se asociará con el agente de la consola.
   b. Introduzca un nombre para el sistema.
   c. En **¿Está ejecutando en un entorno seguro?** mantenga el modo restringido deshabilitado.

      El modo restringido no es compatible cuando el agente de consola está instalado localmente.

   d. Seleccione **Comencemos**.

Proporcionar credenciales del proveedor de nube a la NetApp Console

Después de instalar y configurar el agente de consola, agregue sus credenciales de nube para que el agente de consola tenga los permisos necesarios para realizar acciones en AWS o Azure.

AWS

Antes de empezar

Si acaba de crear estas credenciales de AWS, es posible que tarden unos minutos en estar disponibles. Espere unos minutos antes de agregar las credenciales a la consola.

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**.

Ya puedes ir a la "NetApp Console" para comenzar a utilizar el agente de consola.

Azur

Antes de empezar

Si acaba de crear estas credenciales de Azure, es posible que tarden unos minutos en estar disponibles. Espere unos minutos antes de agregar las credenciales del agente de consola.

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

El agente de consola ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre. Ya puedes ir a la "NetApp Console" para comenzar a utilizar el agente de consola.

Instalar un agente de consola local mediante VCenter

Si es un usuario de VMWare, puede utilizar un OVA para instalar un agente de consola en su VCenter. La descarga o URL de OVA está disponible a través de la NetApp Console.

Cuando instala un agente de consola con sus herramientas VCenter, puede usar la consola web de la máquina virtual para realizar tareas de mantenimiento."Obtenga más información sobre la consola de VM para el agente."

Prepárese para instalar el agente de consola

Antes de la instalación, asegúrese de que su host de VM cumpla con los requisitos y que el agente de consola pueda acceder a Internet y a las redes de destino. Para utilizar los servicios de datos de NetApp o Cloud Volumes ONTAP, cree credenciales de proveedor de nube para que el agente de la consola realice acciones en su nombre.

Revisar los requisitos del host del agente de la consola

Asegúrese de que su máquina host cumpla con los requisitos de instalación antes de instalar el agente de consola.

- CPU: 8 núcleos u 8 vCPU
- RAM: 32 GB
- Espacio en disco: 165 GB (aprovisionamiento grueso)
- vSphere 7.0 o superior
- Host ESXi 7.03 o superior

Instale el agente en un entorno de vCenter en lugar de hacerlo directamente en un host ESXi.

Configurar el acceso a la red para el agente de la consola

Trabaje con su administrador de red para garantizar que el agente de la consola tenga acceso saliente a los puntos finales y conexiones necesarios a las redes específicas.

Conexiones a redes de destino

El agente de consola requiere una conexión de red a la ubicación donde planea crear y administrar sistemas. Por ejemplo, la red donde planea crear sistemas Cloud Volumes ONTAP o un sistema de almacenamiento en su entorno local.

Acceso a Internet de salida

La ubicación de red donde implementa el agente de consola debe tener una conexión a Internet saliente para comunicarse con puntos finales específicos.

Puntos finales contactados desde computadoras al usar la NetApp Console basada en web

Las computadoras que acceden a la consola desde un navegador web deben tener la capacidad de comunicarse con varios puntos finales. Necesitará usar la consola para configurar el agente de la consola y para el uso diario de la consola.

"Preparar la red para la consola de NetApp" .

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

No puedes administrar recursos en Google Cloud con un agente de consola instalado en tus instalaciones. Para administrar los recursos de Google Cloud, instale un agente en Google Cloud.

AWS

Cuando el agente de consola está instalado localmente, necesita acceso de red a los siguientes puntos finales de AWS para administrar los sistemas NetApp (como Cloud Volumes ONTAP) implementados en AWS.

Puntos finales contactados desde el agente de la consola

El agente de la consola requiere acceso a Internet saliente para comunicarse con los siguientes puntos finales para administrar recursos y procesos dentro de su entorno de nube pública para las operaciones diarias.

Los puntos finales enumerados a continuación son todas entradas CNAME.

Puntos finales	Objetivo
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 .
\ 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.

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://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.

Azur

Cuando el agente de consola está instalado localmente, necesita acceso de red a los siguientes puntos de conexión de Azure para administrar los sistemas NetApp (como Cloud Volumes ONTAP) implementados en Azure.

Puntos finales	Objetivo
\ 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.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
\ 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.

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"

Crear permisos de nube de agente de consola para AWS o Azure

Si desea utilizar los servicios de datos de NetApp en AWS o Azure con un agente de consola local, deberá configurar permisos en su proveedor de nube para poder agregar las credenciales al agente de consola después de instalarlo.

No puedes administrar recursos en Google Cloud con un agente de consola instalado en tus instalaciones. Si desea administrar los recursos de Google Cloud, debe instalar un agente en Google Cloud.

AWS

Para los agentes de consola locales, proporcione permisos de AWS agregando claves de acceso de usuario de IAM.

Utilice claves de acceso de usuario de IAM para agentes de consola locales; los roles de IAM no son compatibles con agentes de consola locales.

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 necesite 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.

Resultado

Ahora debería tener claves de acceso de usuario de IAM con los permisos necesarios. Después de instalar el agente de la consola, asocie estas credenciales con el agente de la consola desde la consola.

Azur

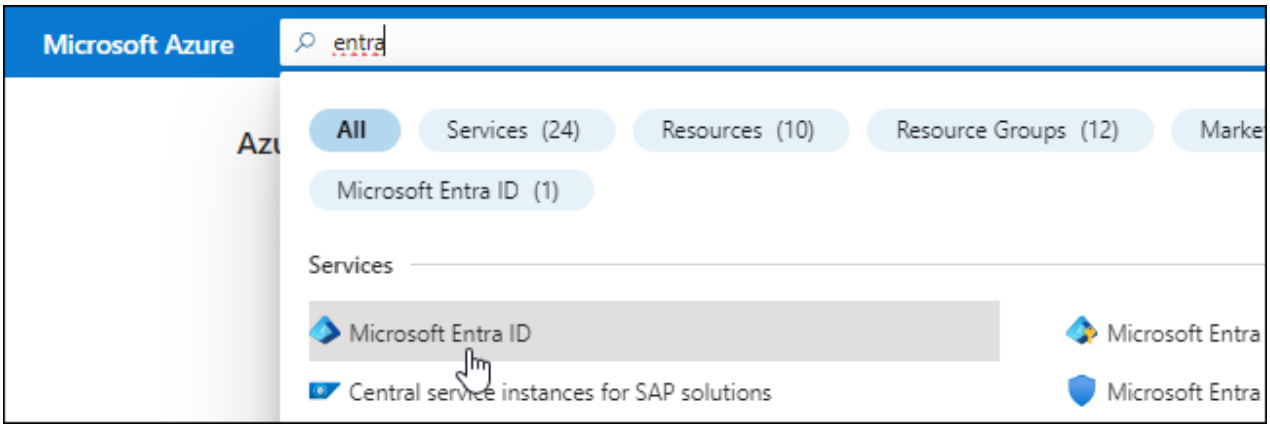
Cuando el agente de consola está instalado localmente, debe otorgarle permisos de Azure configurando una entidad de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que necesita el agente de consola.

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 .

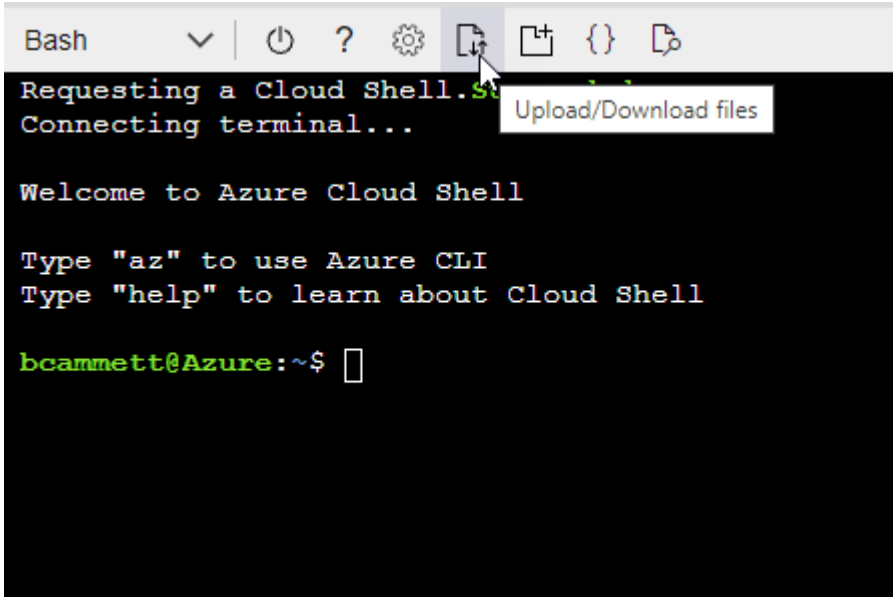
      Ejemplo

      ```
      "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:

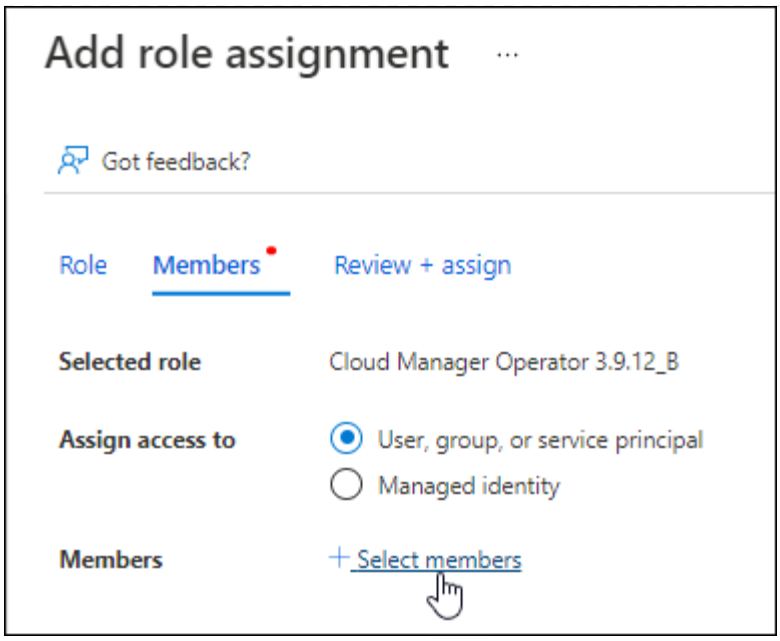
```
az role definition create --role-definition agent_Policy.json
```

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:

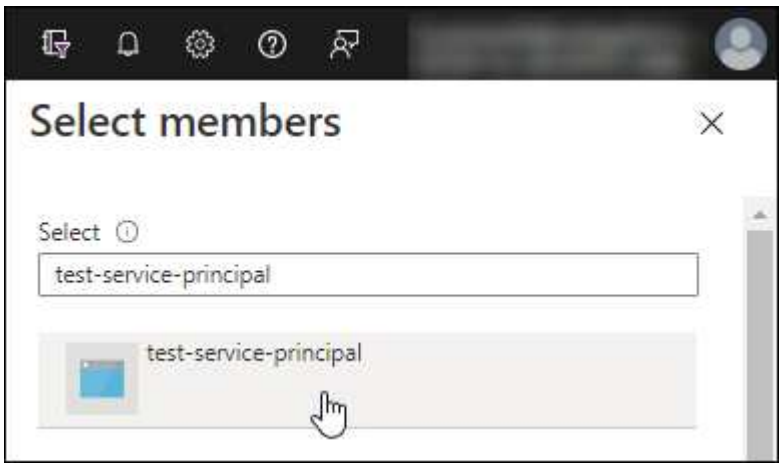
   a. Desde el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de rol**.
   d. En la pestaña **Rol**, seleccione el rol **Operador de consola** y seleccione **Siguiente**.
   e. En la pestaña **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**.

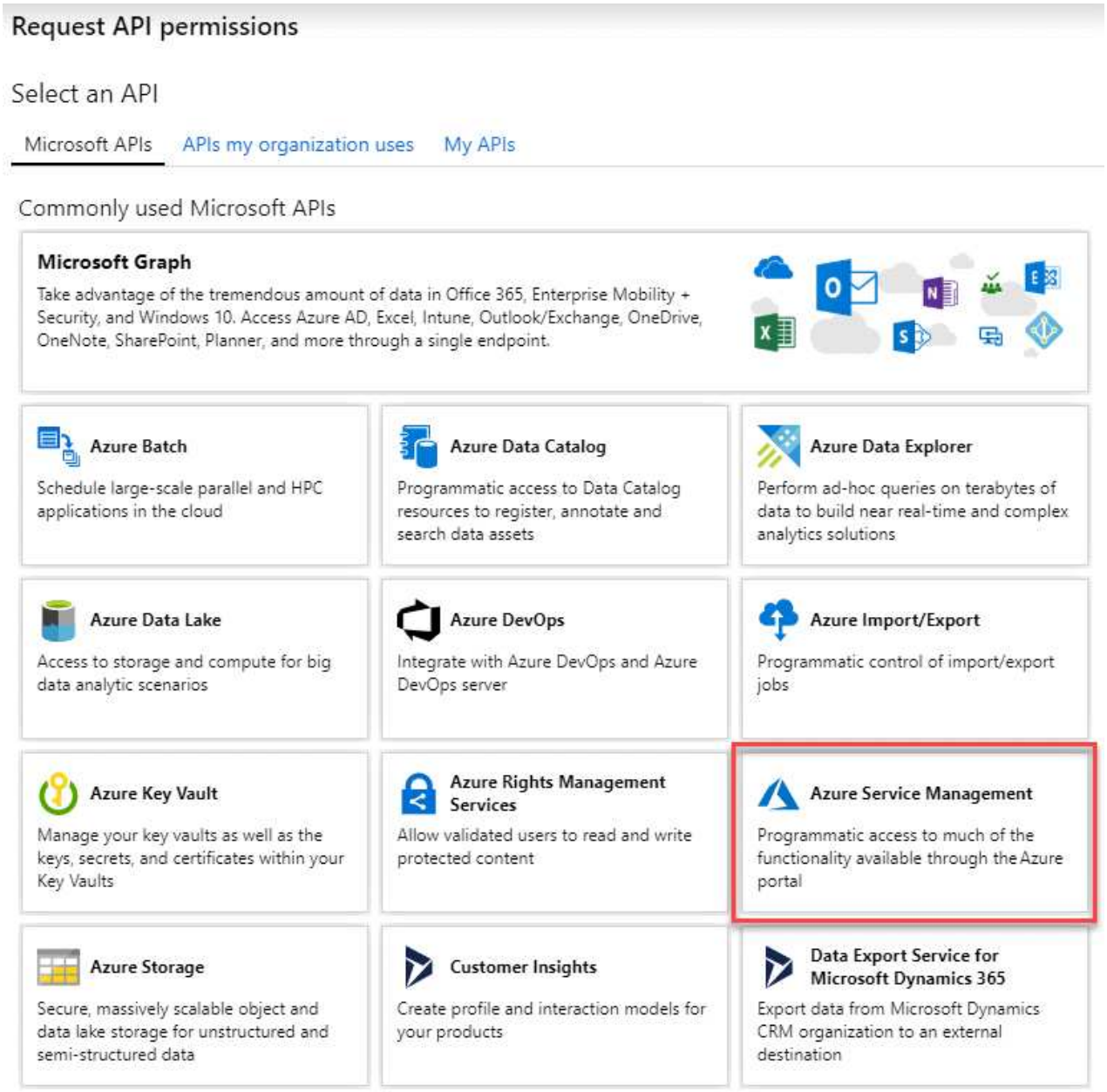
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

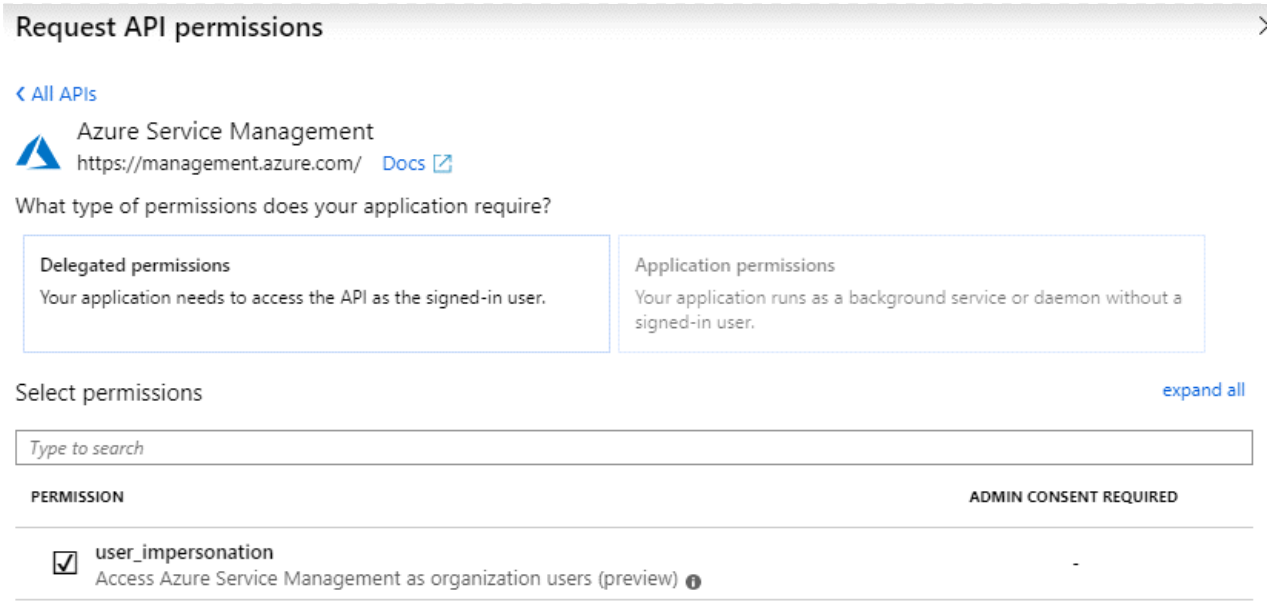
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

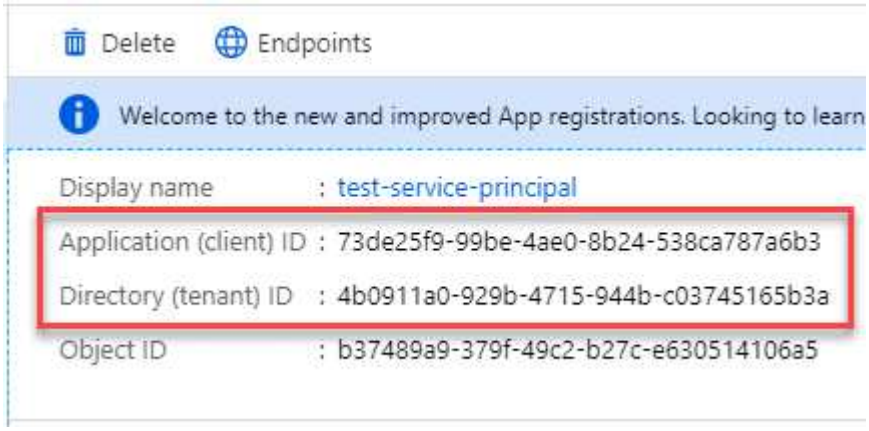


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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

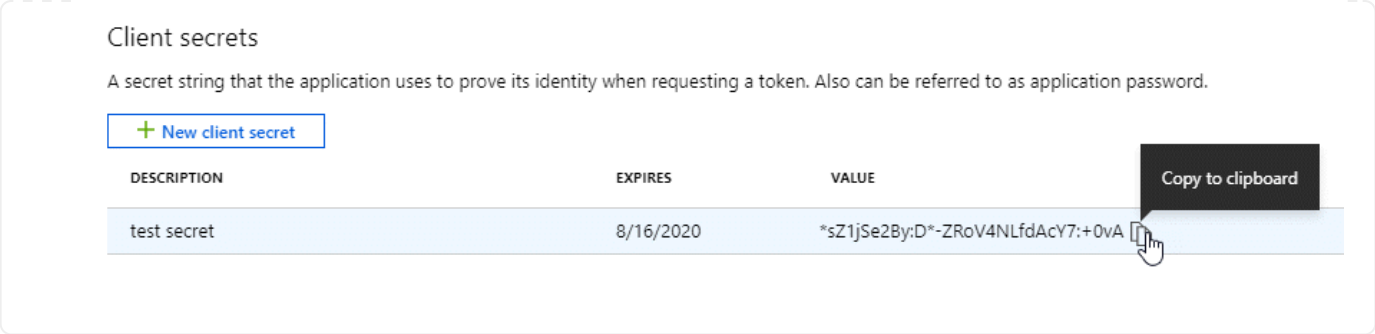
1. En el servicio **Microsoft Entra ID**, seleccione **Registros de aplicaciones** y seleccione la aplicación.
2. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)**.



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.



Instalar un agente de consola en su entorno de VCenter

NetApp admite la instalación del agente de consola en su entorno de VCenter. El archivo OVA incluye una imagen de VM preconfigurada que puede implementar en su entorno VMware. La descarga de un archivo o la implementación de una URL está disponible directamente desde la NetApp Console. Incluye el software del agente de consola y un certificado autofirmado.

Descargue el OVA o copie la URL

Descargue el OVA o copie la URL del OVA directamente desde la NetApp Console.

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione **Implementar agente > Local**.
3. Seleccionar **Con OVA**.
4. Elija descargar el OVA o copiar la URL para usar en VCenter.

Implementar el agente en su VCenter

Inicie sesión en su entorno de VCenter para implementar el agente.

Pasos

1. Cargue el certificado autofirmado en sus certificados de confianza si su entorno lo requiere. Reemplace este certificado después de la instalación."Aprenda cómo reemplazar el certificado autofirmado."
2. Implemente el OVA desde la biblioteca de contenido o el sistema local.

Desde el sistema local	De la biblioteca de contenidos
a. Haga clic derecho y seleccione **Implementar plantilla OVF…**. b. Seleccione el archivo OVA desde la URL o busque su ubicación y seleccione **Siguiente**.	a. Vaya a su biblioteca de contenido y seleccione el OVA del agente de consola. b. Seleccione **Acciones** > **Nueva máquina virtual de esta plantilla**.

3. Complete el asistente Implementar plantilla OVF para implementar el agente de consola.
4. Seleccione un nombre y una carpeta para la máquina virtual, luego seleccione **Siguiente**.
5. Seleccione un recurso computacional y luego seleccione **Siguiente**.
6. Revise los detalles de la plantilla, luego seleccione **Siguiente**.
7. Acepte el acuerdo de licencia y luego seleccione **Siguiente**.
8. Elija el tipo de configuración de proxy que desea utilizar: proxy explícito, proxy transparente o sin proxy.
9. Seleccione el almacén de datos donde desea implementar la máquina virtual y luego seleccione

Siguiente. Asegúrese de que cumpla con los requisitos del host.

10. Seleccione la red a la que desea conectar la VM y luego seleccione **Siguiente**. Asegúrese de que la red sea IPv4 y tenga acceso a Internet saliente a los puntos finales requeridos.
11. En la ventana **Personalizar plantilla**, complete los siguientes campos:
    - **Información del proxy**
      - Si seleccionó proxy explícito, ingrese el nombre de host o la dirección IP del servidor proxy y el número de puerto, así como el nombre de usuario y la contraseña.
      - Si seleccionó un proxy transparente, cargue el certificado correspondiente.
    - **Configuración de máquina virtual**
      - **Omitir verificación de configuración**: esta casilla de verificación no está marcada de manera predeterminada, lo que significa que el agente ejecuta una verificación de configuración para validar el acceso a la red.
        - NetApp recomienda dejar esta casilla sin marcar para que la instalación incluya una comprobación de configuración del agente. La verificación de configuración valida que el agente tenga acceso a la red a los puntos finales requeridos. Si la implementación falla debido a problemas de conectividad, puede acceder al informe de validación y a los registros desde el host del agente. En algunos casos, si está seguro de que el agente tiene acceso a la red, puede optar por omitir la verificación. Por ejemplo, si todavía estás usando el"puntos finales anteriores" utilizado para actualizaciones de agente, la validación falla con un error. Para evitar esto, marque la casilla de verificación para instalar sin una comprobación de validación. "Aprenda a actualizar su lista de puntos finales" .
      - **Contraseña de mantenimiento**: Establezca la contraseña para el `maint` usuario que permite el acceso a la consola de mantenimiento del agente.
      - **Servidores NTP**: especifique uno o más servidores NTP para la sincronización horaria.
      - **Nombre de host**: establece el nombre de host para esta máquina virtual. No debe incluir el dominio de búsqueda. Por ejemplo, un FQDN de console10.searchdomain.company.com debe ingresarse como console10.
      - **DNS principal**: especifique el servidor DNS principal que se utilizará para la resolución de nombres.
      - **DNS secundario**: especifique el servidor DNS secundario que se utilizará para la resolución de nombres.
      - Dominios de búsqueda: especifique el nombre de dominio de búsqueda que se utilizará al resolver el nombre de host. Por ejemplo, si el FQDN es console10.searchdomain.company.com, ingrese searchdomain.company.com.
      - **Dirección IPv4**: la dirección IP que se asigna al nombre de host.
      - **Máscara de subred IPv4**: La máscara de subred para la dirección IPv4.
      - **Dirección de puerta de enlace IPv4**: la dirección de puerta de enlace para la dirección IPv4.
12. Seleccione **Siguiente**.
13. Revise los detalles en la ventana **Listo para completar**, seleccione **Finalizar**.

    La barra de tareas de vSphere muestra el progreso a medida que se implementa el agente de consola.
14. Encienda la máquina virtual.

Si la implementación falla, puede acceder al informe de validación y a los registros desde el host del agente."Aprenda a solucionar problemas de instalación."

Registrar el agente de consola con NetApp Console

Inicie sesión en la consola y asocie el agente de la consola con su organización. La forma de iniciar sesión depende del modo en que esté utilizando la Consola. Si está utilizando la consola en modo estándar, inicie sesión a través del sitio web de SaaS. Si está utilizando la consola en modo restringido o privado, inicie sesión localmente desde el host del agente de la consola.

Pasos

1. Abra un navegador web e ingrese la URL del host del agente de la consola:

   La URL del host de la consola puede ser un host local, una dirección IP privada o una dirección IP pública, según la configuración del host. Por ejemplo, si el agente de la consola está en la nube pública sin una dirección IP pública, debe ingresar una dirección IP privada de un host que tenga una conexión al host del agente de la consola.

2. Regístrate o inicia sesión.
3. Después de iniciar sesión, configure la consola:
   a. Especifique la organización de la consola que se asociará con el agente de la consola.
   b. Introduzca un nombre para el sistema.
   c. En **¿Está ejecutando en un entorno seguro?** mantenga el modo restringido deshabilitado.

      El modo restringido no es compatible cuando el agente de consola está instalado localmente.

   d. Seleccione **Comencemos**.

Agregar credenciales del proveedor de la nube a la consola

Después de instalar y configurar el agente de consola, agregue sus credenciales de nube para que el agente de consola tenga los permisos necesarios para realizar acciones en AWS o Azure.

AWS

Antes de empezar

Si acaba de crear estas credenciales de AWS, es posible que tarden unos minutos en estar disponibles. Espere unos minutos antes de agregar las credenciales a la consola.

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**.

Ya puedes ir a la "NetApp Console" para comenzar a utilizar el agente de consola.

Azur

Antes de empezar

Si acaba de crear estas credenciales de Azure, es posible que tarden unos minutos en estar disponibles. Espere unos minutos antes de agregar las credenciales del agente de consola.

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

El agente de consola ahora tiene los permisos que necesita para realizar acciones en Azure en su nombre. Ya puedes ir a la "NetApp Console" para comenzar a utilizar el agente de consola.

Puertos para el agente de consola local

El agente de consola utiliza puertos *entrantes* cuando se instala manualmente en un host Linux local. Consulte estos puertos para fines de planificación.

Estas reglas de entrada se aplican a todos los modos de implementación de la NetApp Console .

Protocolo	Puerto	Objetivo
HTTP	80	• Proporciona acceso HTTP desde los navegadores web del cliente a la interfaz de usuario local • Se utiliza durante el proceso de actualización de Cloud Volumes ONTAP
HTTPS	443	Proporciona acceso HTTPS desde los navegadores web del cliente a la interfaz de usuario local

Mantener agentes de consola

Mantener un host VCenter o ESXi para el agente de consola

Puede realizar cambios en su host VCenter o ESXi existente después de implementar el agente de consola. Por ejemplo, puede aumentar la CPU o la RAM de la instancia de VM que aloja el agente de consola.

Realice estas tareas de mantenimiento mediante la consola web de la máquina virtual:

- Aumentar el tamaño del disco
- Reiniciar el agente
- Actualizar rutas estáticas
- Actualizar dominios de búsqueda

Limitaciones

Aún no se admite la actualización del agente a través de la consola. Además, solo puedes ver información sobre la dirección IP, DNS y puertas de enlace.

Acceder a la consola de mantenimiento de la máquina virtual

Puede acceder a la consola de mantenimiento desde el cliente VSphere.

Pasos

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.
3. Seleccione **Iniciar consola web**.
4. Inicie sesión en la instancia de VM utilizando el nombre de usuario y la contraseña que especificó cuando creó la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste cuando creaste la instancia de VM.

Cambiar la contraseña del usuario principal

Puede cambiar la contraseña de la `maint` usuario.

Pasos

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.
3. Seleccione **Iniciar consola web**.
4. Inicie sesión en la instancia de VM utilizando el nombre de usuario y la contraseña que especificó cuando creó la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste cuando creaste la instancia de VM.
5. Ingresar `1` Para ver el `System Configuration` menú.
6. Ingresar `1` para cambiar la contraseña del usuario de mantenimiento y seguir las instrucciones en pantalla.

Aumente la CPU o RAM de la instancia de VM

Puede aumentar la CPU o la RAM de la instancia de VM que aloja el agente de consola.

Edite la configuración de la instancia de VM en su host VCenter o ESXi y luego use la consola de mantenimiento para aplicar los cambios.

Pasos en el cliente VSphere

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.
3. Haga clic derecho en la instancia de VM y seleccione **Editar configuración**.
4. Aumente el espacio del disco duro utilizado para la partición /opt o /var.
   a. Seleccione **Disco duro 2** para aumentar el espacio del disco duro utilizado para /opt.
   b. Seleccione **Disco duro 3** para aumentar el espacio del disco duro utilizado para /var.
5. Guarde sus cambios.

Pasos en la consola de mantenimiento

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.
3. Seleccione **Iniciar consola web**.
4. Inicie sesión en la instancia de VM utilizando el nombre de usuario y la contraseña que especificó cuando creó la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste cuando creaste la instancia de VM.
5. Ingresar `1 to view the `System Configuration` menú.
6. Ingresar `2` y siga las instrucciones en pantalla. La consola busca nuevas configuraciones y aumenta el tamaño de las particiones.

Ver la configuración de red para la máquina virtual del agente

Vea la configuración de red de la máquina virtual del agente en el cliente VSphere para confirmar o solucionar problemas de red. Solo puede ver (no actualizar) las siguientes configuraciones de red: dirección IP y detalles de DNS.

Pasos

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.

3. Seleccione **Iniciar consola web**.
4. Inicie sesión en la instancia de VM utilizando el nombre de usuario y la contraseña que especificó cuando creó la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste cuando creaste la instancia de VM.
5. Ingresar `2` Para ver el `Network Configuration` menú.
6. Introduzca un número entre 1 y 6 para ver la configuración de red correspondiente.

Actualizar las rutas estáticas para la máquina virtual del agente

Agregue, actualice o elimine rutas estáticas para la máquina virtual del agente según sea necesario.

Pasos

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.
3. Seleccione **Iniciar consola web**.
4. Inicie sesión en la instancia de VM utilizando el nombre de usuario y la contraseña que especificó cuando creó la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste cuando creaste la instancia de VM.
5. Ingresar `2` Para ver el `Network Configuration` menú.
6. Ingresar `7` para actualizar rutas estáticas y seguir las instrucciones en pantalla.
7. Presione Enter.
8. Opcionalmente, realice cambios adicionales.
9. Ingresar `9` para confirmar sus cambios.

Actualizar la configuración de búsqueda de dominio para la máquina virtual del agente

Puede actualizar la configuración del dominio de búsqueda para la máquina virtual del agente.

Pasos

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.
3. Seleccione **Iniciar consola web**.
4. Inicie sesión en la instancia de VM utilizando el nombre de usuario y la contraseña que especificó cuando creó la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste cuando creaste la instancia de VM.
5. Ingresar `2`` Para ver el `Network Configuration` menú.
6. Ingresar `8` para actualizar la configuración de búsqueda del dominio y seguir las instrucciones en pantalla.
7. Presione Enter.
8. Opcionalmente, realice cambios adicionales.
9. Ingresar `9` para confirmar sus cambios.

Acceda a las herramientas de diagnóstico del agente

Acceda a herramientas de diagnóstico para solucionar problemas con el agente de la consola. Es posible que

el soporte de NetApp le solicite que haga esto al solucionar problemas.

Pasos

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.
3. Seleccione **Iniciar consola web**.
4. Inicie sesión en la instancia de VM utilizando el nombre de usuario y la contraseña que especificó cuando creó la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste cuando creaste la instancia de VM.
5. Ingresar `3` para ver el menú de Soporte y Diagnóstico.
6. Ingresar `1` para acceder a las herramientas de diagnóstico y seguir las instrucciones en pantalla. + Por ejemplo, puede verificar que todos los servicios del agente se estén ejecutando. "Comprobar el estado del agente de la consola" .

Acceda a las herramientas de diagnóstico del agente de forma remota

Puede acceder a herramientas de diagnóstico de forma remota con una herramienta como Putty. Habilite el acceso SSH a la máquina virtual del agente asignando una contraseña de un solo uso.

El acceso SSH permite funciones de terminal avanzadas como copiar y pegar.

Pasos

1. Abra el cliente VSphere e inicie sesión en su VCenter.
2. Seleccione la instancia de VM que aloja el agente de consola.
3. Seleccione **Iniciar consola web**.
4. Inicie sesión en la instancia de VM utilizando el nombre de usuario y la contraseña que especificó cuando creó la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste cuando creaste la instancia de VM.
5. Ingresar `3` Para ver el `Support and Diagnostics` menú.
6. Ingresar `2` para acceder a las herramientas de diagnóstico y seguir las instrucciones en pantalla para configurar una contraseña de un solo uso que vence en 24 horas.
7. Utilice una herramienta SSH como Putty para conectarse a la máquina virtual del agente usando el nombre de usuario `diag` y la contraseña de un solo uso que usted configuró.

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

Cuando utiliza la NetApp Console en modo restringido, se puede acceder a la interfaz de usuario desde la máquina virtual del agente de la consola que está implementada en su región de nube o en sus instalaciones. De forma predeterminada, la consola utiliza un certificado SSL autofirmado para proporcionar acceso HTTPS seguro a la consola basada en web que se ejecuta en el agente de la consola.

Si su negocio lo requiere, puede instalar un certificado firmado por una autoridad de certificación (CA), que proporciona una mejor protección de seguridad que un certificado autofirmado. Después de instalar el certificado, la consola utiliza el certificado firmado por la CA cuando los usuarios acceden a la consola basada en web.

Instalar un certificado HTTPS

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

Acerca de esta tarea

Puede instalar el certificado utilizando una de las siguientes opciones:

- Genere una solicitud de firma de certificado (CSR) desde la consola, envíe la solicitud de certificado a una CA y luego instale el certificado firmado por la CA en el agente de la consola.

  El par de claves que utiliza la consola para generar la CSR se almacena internamente en el agente de la consola. La consola recupera automáticamente el mismo par de claves (clave privada) cuando instala el certificado en el agente de la consola.

- Instale un certificado firmado por CA que ya tenga.

  Con esta opción, el CSR no se genera a través de la Consola. Genera la CSR por separado y almacena la clave privada externamente. Proporciona a la consola la clave privada cuando instala el certificado.

Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione el menú de acciones para un agente de consola y seleccione **Configuración HTTPS**.

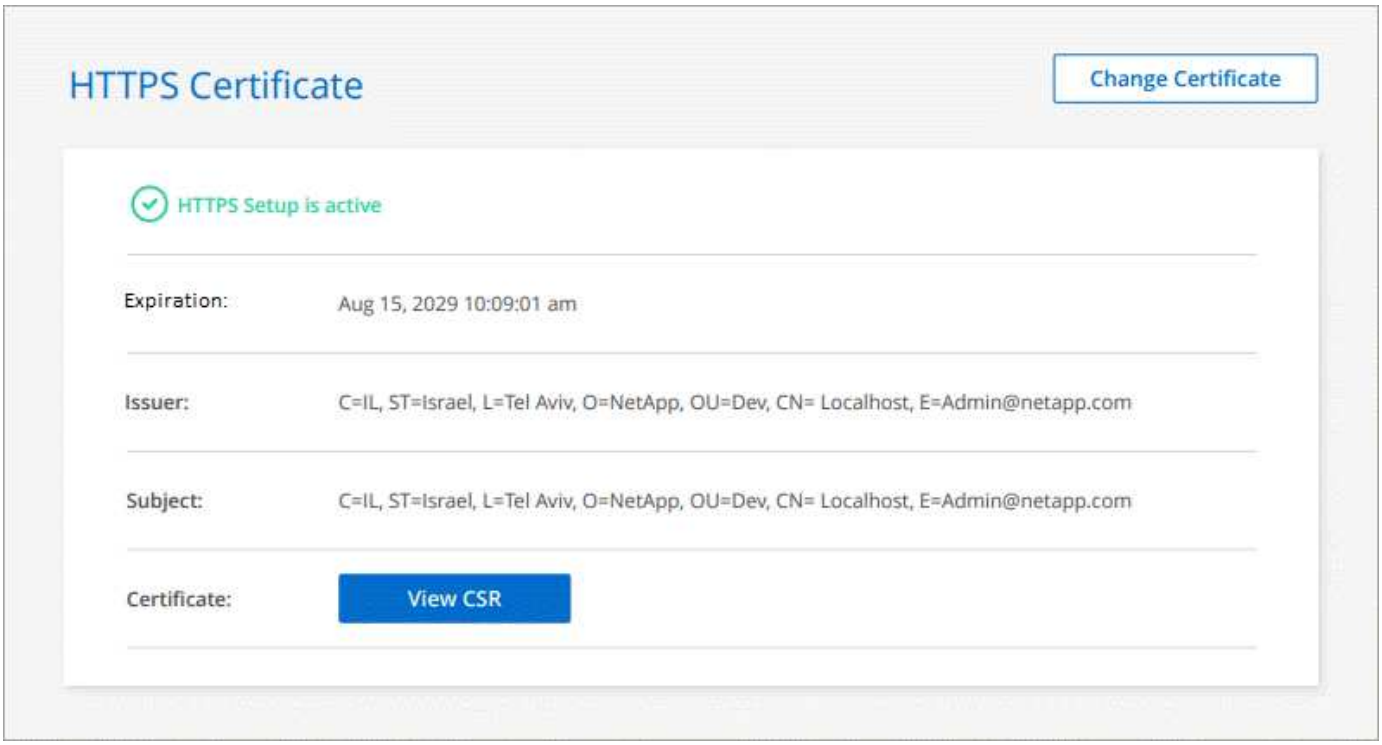
   El agente de la consola debe estar conectado para editarlo.

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

Opción	Descripción
Generar un CSR	a. Ingrese el nombre de host o DNS del host del agente de consola (su nombre común) y luego seleccione **Generar CSR**. La consola muestra una solicitud de firma de certificado. b. Utilice la CSR para enviar una solicitud de certificado SSL a una CA. El certificado debe utilizar el formato X.509 codificado en Base-64 de correo de privacidad mejorada (PEM). c. Cargue el archivo del certificado y luego seleccione **Instalar**.
Instale su propio certificado firmado por CA	a. Seleccione **Instalar certificado firmado por CA**. b. Cargue el archivo del certificado y la clave privada y luego seleccione **Instalar**. El certificado debe utilizar el formato X.509 codificado en Base-64 de correo de privacidad mejorada (PEM).

Resultado

El agente de consola ahora utiliza el certificado firmado por CA para proporcionar acceso HTTPS seguro. La siguiente imagen muestra un agente configurado para acceso seguro:



Renovar el certificado HTTPS de la consola

Debe renovar el certificado HTTPS del agente antes de que caduque para garantizar un acceso seguro. Si no renueva el certificado antes de que caduque, aparecerá una advertencia cuando los usuarios accedan a la consola web mediante HTTPS.

Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione el menú de acciones para un agente de consola y seleccione **Configuración HTTPS**.

   Se muestran detalles sobre el certificado, incluida la fecha de vencimiento.

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

Configurar un agente de consola para utilizar un servidor proxy

Si sus políticas corporativas requieren que utilice un servidor proxy para todas las comunicaciones a Internet, entonces deberá configurar sus agentes para utilizar ese servidor proxy. Si no configuró un agente de consola para usar un servidor proxy durante la instalación, puede configurar el agente de consola para usar ese servidor proxy en cualquier momento.

El servidor proxy del agente permite el acceso saliente a Internet sin una IP pública o una puerta de enlace NAT. El servidor proxy proporciona conectividad saliente solo para el agente de la consola, no para los sistemas Cloud Volumes ONTAP .

Si los sistemas Cloud Volumes ONTAP carecen de acceso a Internet saliente, la consola los configura para utilizar el servidor proxy del agente de la consola. Debe asegurarse de que el grupo de seguridad del agente de la consola permita conexiones entrantes a través del puerto 3128. Abra este puerto después de implementar el agente de consola.

Si el agente de la consola no tiene una conexión a Internet saliente, los sistemas Cloud Volumes ONTAP no pueden usar el servidor proxy configurado.

Configuraciones compatibles

- Los servidores proxy transparentes son compatibles con los agentes que prestan servicio a los sistemas Cloud Volumes ONTAP . Si utiliza servicios de datos de NetApp con Cloud Volumes ONTAP, cree un agente dedicado para Cloud Volumes ONTAP donde pueda usar un servidor proxy transparente.
- Los servidores proxy explícitos son compatibles con todos los agentes, incluidos aquellos que administran sistemas Cloud Volumes ONTAP y aquellos que administran servicios de datos de NetApp .
- HTTP y HTTPS.
- El servidor proxy puede residir en la nube o en su red.

Una vez que haya configurado un proxy, no podrá cambiar el tipo de proxy. Si necesita cambiar el tipo de proxy, elimine el agente de consola y agregue un nuevo agente con el nuevo tipo de proxy.

Habilitar un proxy explícito en un agente de consola

Cuando configura un agente de consola para usar un servidor proxy, ese agente y los sistemas Cloud Volumes ONTAP que administra (incluido cualquier mediador de HA) usan el servidor proxy.

Esta operación reinicia el agente de consola. Verifique que el agente de la consola esté inactivo antes de continuar.

Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione el menú de acciones para un agente de consola y seleccione **Editar agente**.

   El agente de la consola debe estar activo para editarlo.

3. Seleccione **Configuración de proxy HTTP**.
4. Seleccione **Proxy explícito** en el campo Tipo de configuración.
5. Seleccione **Habilitar proxy**.
6. Especifique el servidor utilizando la sintaxis http://address:port o https://address:port
7. Especifique un nombre de usuario y una contraseña si se requiere autenticación básica para el servidor.

   Tenga en cuenta lo siguiente:

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

Por ejemplo: netapp%92proxy

- La consola no admite contraseñas que incluyan el carácter @.

8. Seleccione **Guardar**.

Habilitar un proxy transparente para un agente de consola

Solo Cloud Volumes ONTAP admite el uso de un proxy transparente en el agente de la consola. Si utiliza servicios de datos de NetApp además de Cloud Volumes ONTAP, debe crear un agente independiente para utilizarlo con los servicios de datos o con Cloud Volumes ONTAP.

Antes de habilitar un proxy transparente, asegúrese de que se cumplan los siguientes requisitos:

- El agente está instalado en la misma red que el servidor proxy transparente.
- La inspección TLS está habilitada en el servidor proxy.
- Tienes un certificado en formato PEM que coincide con el utilizado en el servidor proxy transparente.
- No utilice el agente de consola para ningún servicio de datos de NetApp que no sea Cloud Volumes ONTAP.

Para configurar un agente existente para que utilice un servidor proxy transparente, utilice la herramienta de mantenimiento del agente de consola que está disponible a través de la línea de comandos en el host del agente de consola.

Cuando se configura un servidor proxy, el agente de la consola se reinicia. Verifique que el agente de la consola esté inactivo antes de continuar.

Pasos

Asegúrese de tener un archivo de certificado en formato PEM para el servidor proxy. Si no tiene un certificado, comuníquese con su administrador de red para obtener uno.

1. Abra una interfaz de línea de comandos en el host del agente de la consola.
2. Navegue hasta el directorio de la herramienta de mantenimiento del agente de la consola: `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Ejecute el siguiente comando para habilitar el proxy transparente, donde `/home/ubuntu/<certificate-file>.pem` es el directorio y el nombre del archivo de certificado que tiene para el servidor proxy:

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Asegúrese de que el archivo del certificado esté en formato PEM y resida en el mismo directorio que el comando o especifique la ruta completa al archivo del certificado.

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Modificar el proxy transparente para el agente de la consola

Puede actualizar el servidor proxy transparente existente de un agente de consola mediante el `proxy update` comando o elimine el servidor proxy transparente mediante el uso del `proxy remove` dominio. Para

obtener más información, revise la documentación de"Consola de mantenimiento del agente" .

> Una vez que haya configurado un proxy, no podrá cambiar el tipo de proxy. Si necesita cambiar el tipo de proxy, elimine el agente de consola y agregue un nuevo agente con el nuevo tipo de proxy.

Actualice el proxy del agente de la consola si pierde el acceso a Internet

Si la configuración del proxy de su red cambia, su agente podría perder el acceso a Internet. Por ejemplo, si alguien cambia la contraseña del servidor proxy o actualiza el certificado. En este caso, necesitarás acceder a la interfaz de usuario directamente desde el host del agente de la consola y actualizar la configuración. Asegúrese de tener acceso a la red del host del agente de la consola y de que pueda iniciar sesión en la consola.

Habilitar el tráfico directo de API

Si configuró un agente de consola para usar un servidor proxy, puede habilitar el tráfico de API directo en el agente de consola para enviar llamadas de API directamente a los servicios del proveedor de la nube sin pasar por el proxy. Los agentes que se ejecutan en AWS, Azure o Google Cloud admiten esta opción.

Si deshabilita Azure Private Links con Cloud Volumes ONTAP y usa puntos de conexión de servicio, habilite el tráfico de API directo. De lo contrario, el tráfico no se enrutará correctamente.

"Obtenga más información sobre el uso de Azure Private Link o puntos de conexión de servicio con Cloud Volumes ONTAP"

Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Descripción general**, seleccione el menú de acciones para un agente de consola y seleccione **Editar agente**.

   El agente de la consola debe estar activo para editarlo.

3. Seleccione **Admitir tráfico API directo**.
4. Seleccione la casilla de verificación para habilitar la opción y luego seleccione **Guardar**.

Solucionar problemas del agente de la consola

Para solucionar problemas con un agente de consola, puede verificar los problemas usted mismo o trabajar con el soporte de NetApp , que podría solicitarle su ID de sistema, la versión del agente o los últimos mensajes de AutoSupport .

Si tiene una cuenta del sitio de soporte de NetApp , también puede ver la"Base de conocimientos de NetApp ."

Mensajes de error comunes y resoluciones

Esta tabla enumera mensajes de error comunes y muestra cómo solucionarlos:

Mensaje de error	Explicación	Qué hacer
No se puede cargar la interfaz de usuario del agente de la consola	La instalación del agente ha fallado	• Verifique que el servicio Service Manager esté activo. • Verifique que todos los contenedores estén ejecutándose. • Asegúrese de que su firewall permita el acceso al servicio en el puerto 8888. • Si aún tienes problemas, contacta con el soporte técnico.
No se puede acceder a la interfaz de usuario del agente de NetApp	Este mensaje aparece al intentar acceder a la dirección IP de un agente. El agente puede fallar al inicializarse si no tiene el acceso a la red correcto o si es inestable.	• Conectarse al agente de la consola. • Verifique que el servicio Service Manager • Verifique que el agente tenga el acceso a la red que necesita."Obtenga más información sobre los puntos finales de acceso a la red necesarios."
No se puede cargar la configuración del agente	La consola muestra este mensaje cuando intenta acceder a la página de configuración del agente.	• Compruebe si el contenedor OCCM está ejecutándose y funcionando. • Si el problema persiste, comuníquese con el soporte técnico.
No se puede cargar información de soporte para el agente.	Este mensaje aparece si el agente no puede acceder a su cuenta de soporte.	• Verifique que el agente tenga acceso saliente a los puntos finales requeridos."Obtenga más información sobre los puntos finales de acceso a la red necesarios."

Comprobar el estado del agente de la consola

Utilice uno de los siguientes comandos para verificar su agente de consola. Todos los servicios deben tener un estado de *En ejecución*. Si este no es el caso, comuníquese con el soporte de NetApp .

Para obtener información más detallada sobre cómo acceder a los diagnósticos del agente de la consola, consulte los siguientes temas:

- "Comprobar el estado del agente de la consola (para implementaciones de host Linux)"
- "Comprobar el estado del agente de la consola (para implementaciones de VCenter)"

Docker (para implementaciones de Ubuntu y VCenter)

```
docker ps -a
```

Podman (para implementaciones de RedHat Enterprise Linux)

```
podman ps -a
```

Ver la versión del agente de la consola

Vea la versión del agente de la consola para confirmar la actualización o compartirla con su representante de NetApp .

Pasos

1. Seleccione **Administración > Soporte > Agentes**.

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

Verificar el acceso a la red

Asegúrese de que el agente de la consola tenga el acceso a la red que necesita."Obtenga más información sobre los puntos de acceso de red necesarios."

Ejecutar comprobaciones de configuración en el agente de la consola

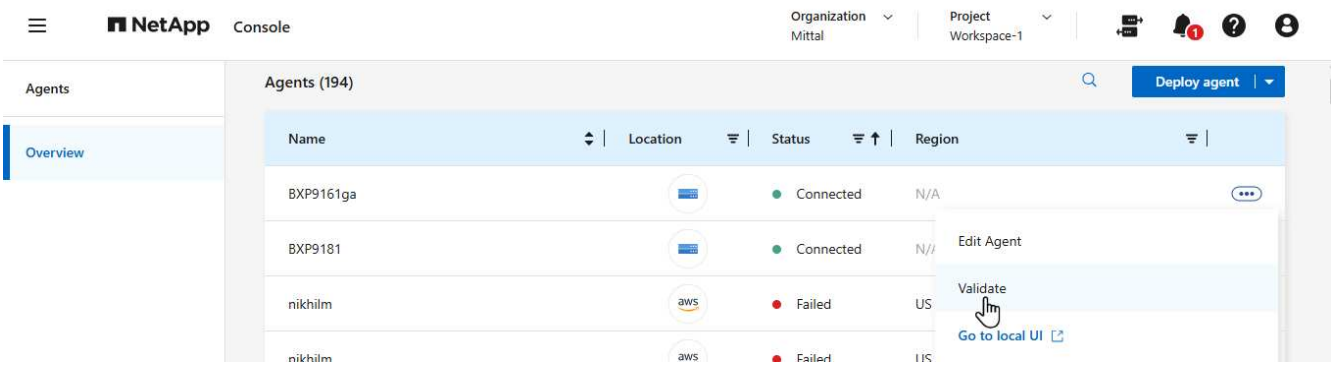
Ejecute comprobaciones de configuración en los agentes de la consola desde la consola o desde la consola de mantenimiento del agente para asegurarse de que estén conectados.

También puede ejecutar comprobaciones de configuración mediante la consola de mantenimiento del agente."Obtenga más información sobre el uso del comando validate de config-checker."

Sólo puedes validar agentes que tengan un estado de **Conectado**.

Pasos desde la consola

1. Seleccione **Administración > Agentes**.
2. Seleccione el menú de acciones de un agente de consola que desee verificar y elija **Validar**.



La validación puede tardar hasta 15 minutos. Los resultados se muestran cuando está terminado.

Problemas de instalación del agente de consola

Si la instalación falla, consulte el informe y los registros para resolver los problemas.

También puede acceder al informe de validación en formato JSON y a los registros de configuración directamente desde el host del agente de la consola en los siguientes directorios:

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- Para las nuevas implementaciones de agentes, NetApp verifica los siguientes puntos finales:"listado aquí" . Esta comprobación de configuración falla con un error si está utilizando los puntos finales anteriores utilizados para las actualizaciones."listado aquí" . NetApp recomienda actualizar sus reglas de firewall para permitir el acceso a los puntos finales actuales y bloquear el acceso a los puntos finales anteriores lo antes posible."Aprenda a actualizar su red" .
- Si actualiza los puntos finales en su firewall, sus agentes existentes continuarán funcionando.

Deshabilitar las comprobaciones de configuración para instalaciones manuales

Puede haber ocasiones en las que necesite deshabilitar las comprobaciones de configuración que verifican la conectividad saliente durante la instalación. Por ejemplo, al instalar manualmente un agente en su entorno de Government Cloud, debe deshabilitar las comprobaciones de configuración o la instalación fallará.

Pasos

Puede deshabilitar la verificación de configuración configurando el indicador *skipConfigCheck* en el archivo *com/opt/application/netapp/service-manager-2/config.json*. De forma predeterminada, esta bandera se establece como falsa y la verificación de configuración verifica el acceso saliente para el agente. Establezca esta bandera como verdadera para deshabilitar la verificación. Familiarícese con la sintaxis JSON antes de completar este paso.

Para volver a habilitar la verificación de configuración, siga estos pasos y configure el indicador *skipConfigCheck* en falso.

Pasos

1. Acceda al host del agente de la consola como root o con privilegios de sudo.
2. Cree una copia de seguridad del archivo */opt/application/netapp/service-manager-2/config.json* para asegurarse de poder revertir los cambios.
3. Detenga el servicio del administrador de servicios 2 ejecutando el siguiente comando:

```
systemctl stop netapp-service-manager.service
```

1. Edite el archivo */opt/application/netapp/service-manager-2/config.json* y cambie el valor del indicador *skipConfigCheck* a verdadero.

```
  "skipConfigCheck": true
```

2. Guarde su archivo.
3. Reinicie el servicio del administrador de servicios 2 ejecutando el siguiente comando:

```
systemctl restart netapp-service-manager.service
```

Trabaje con el soporte de NetApp

Si no ha podido resolver los problemas con su agente de consola, puede comunicarse con el soporte de NetApp . Es posible que el soporte de NetApp le solicite el ID del agente de la consola o que le envíe los registros del agente de la consola si aún no los tiene.

Encuentra el ID del agente de la consola

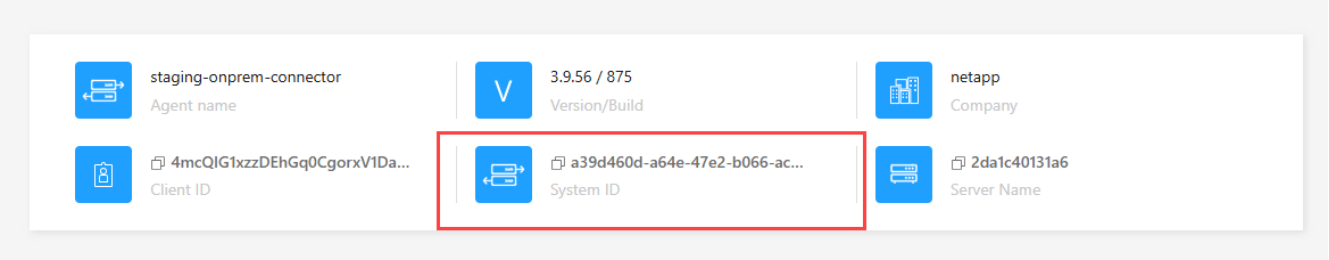
Para ayudarlo a comenzar, es posible que necesite el ID del sistema de su agente de consola. La identificación normalmente se utiliza para fines de licencia y resolución de problemas.

Pasos

1. Seleccione **Administración > Soporte > Agentes**.

   Puede encontrar el ID del sistema en la parte superior de la página.

   Ejemplo



2. Pase el cursor y haga clic sobre el ID para copiarlo.

Descargue o envíe un mensaje de AutoSupport

Si tiene problemas, NetApp podría solicitarle que envíe un mensaje de AutoSupport al soporte de NetApp para solucionar problemas.

La NetApp Console tarda hasta cinco horas en enviar mensajes de AutoSupport debido al equilibrio de carga. Para comunicaciones urgentes, descargue el archivo y envíelo manualmente.

Pasos

1. Seleccione **Administración > Soporte > Agentes**.
2. Dependiendo de cómo necesite enviar la información al soporte de NetApp , elija una de las siguientes opciones:

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

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

Solucionar errores de descarga al usar una puerta de enlace NAT de Google Cloud

El agente de consola descarga automáticamente actualizaciones de software para Cloud Volumes ONTAP. Su configuración puede provocar que la descarga falle si utiliza una puerta de enlace NAT de Google Cloud. Puede corregir este problema limitando la cantidad de partes en que se divide la imagen del software. Este paso debe completarse utilizando la API.

Paso

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

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

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

Tenga en cuenta que 32 es un valor de ejemplo. El valor depende de su configuración NAT y del número de sesiones simultáneas.

"Obtenga más información sobre la llamada API /occm/config"

Obtenga ayuda de la base de conocimientos de NetApp

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

Desinstalar y eliminar un agente de consola

Desinstale un agente de consola para solucionar problemas o eliminarlo permanentemente del host. Los pasos que debes seguir dependen del modo de implementación que estés utilizando. Una vez que haya eliminado un agente de consola de su entorno, puede eliminarlo de la consola.

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

Desinstalar el agente cuando se utiliza el modo estándar o restringido

Si está utilizando el modo estándar o el modo restringido (en otras palabras, el host del agente tiene conectividad saliente), debe seguir los pasos a continuación para desinstalar el agente.

Pasos

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

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

silent ejecuta el script sin solicitar confirmación.

Eliminar agentes de la consola

Si ha eliminado una máquina virtual de agente o ha desinstalado el agente, debe eliminarlo de la lista de agentes en la consola. Después de eliminar una máquina virtual de agente o desinstalar el software del agente, este muestra el estado **Desconectado** en la consola.

Tenga en cuenta lo siguiente sobre la eliminación de un agente de consola:

- Esta acción no elimina la máquina virtual.
- Esta acción no se puede revertir: una vez que elimines un agente de consola, no podrás volver a agregarlo.

Pasos

1. Seleccione **Administración > Agentes**.
2. En la página **Resumen**, seleccione el menú de acciones para un agente desconectado y seleccione **Eliminar agente**.
3. Ingrese el nombre del agente a confirmar y luego seleccione **Eliminar**.

Administrar las credenciales del proveedor de la nube

AWS

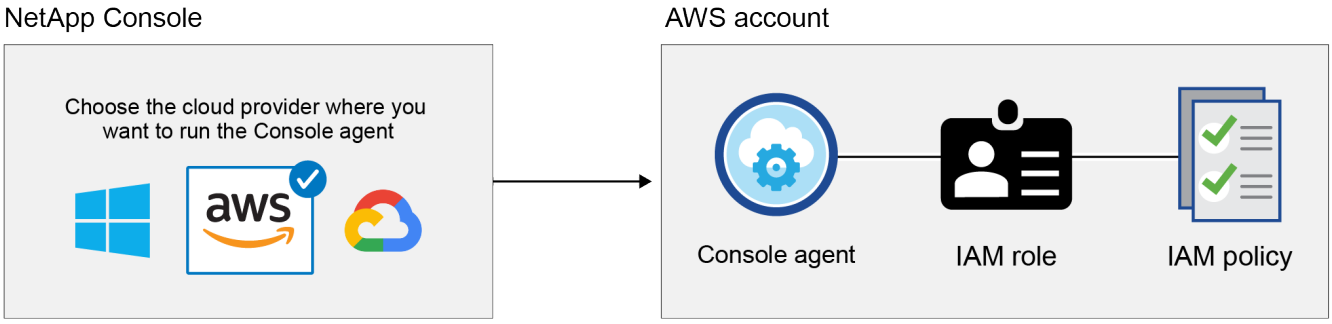
Obtenga información sobre las credenciales y los permisos de AWS en la NetApp Console

Usted administra las credenciales de AWS y las suscripciones al marketplace directamente desde la NetApp Console para garantizar la implementación segura de Cloud Volumes ONTAP y otros servicios de datos, proporcionando las credenciales IAM apropiadas durante la implementación del agente de la consola y asociándolas con las suscripciones de AWS Marketplace para la facturación.

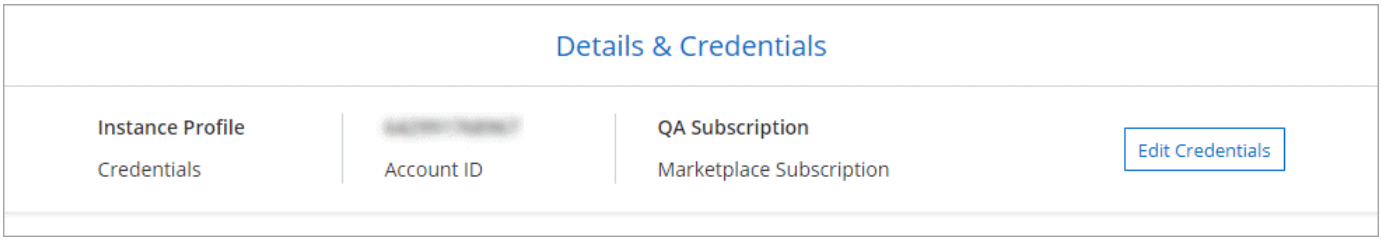
Credenciales iniciales de AWS

Cuando implementa un agente de consola desde la consola, debe proporcionar el ARN de un rol de IAM o claves de acceso para un usuario de IAM. El método de autenticación debe tener permisos para implementar el agente de la consola en AWS. Los permisos necesarios se enumeran en el"Política de despliegue de agentes para AWS" .

Cuando la consola inicia el agente de consola en AWS, crea una función de IAM y un perfil para el agente. También adjunta una política que proporciona al agente de la consola permisos para administrar recursos y procesos dentro de esa cuenta de AWS. "Revisar cómo el Agente utiliza los permisos".



Si agrega un nuevo sistema Cloud Volumes ONTAP , la consola selecciona estas credenciales de AWS de forma predeterminada:



Implemente todos sus sistemas Cloud Volumes ONTAP utilizando las credenciales iniciales de AWS o puede agregar credenciales adicionales.

Credenciales adicionales de AWS

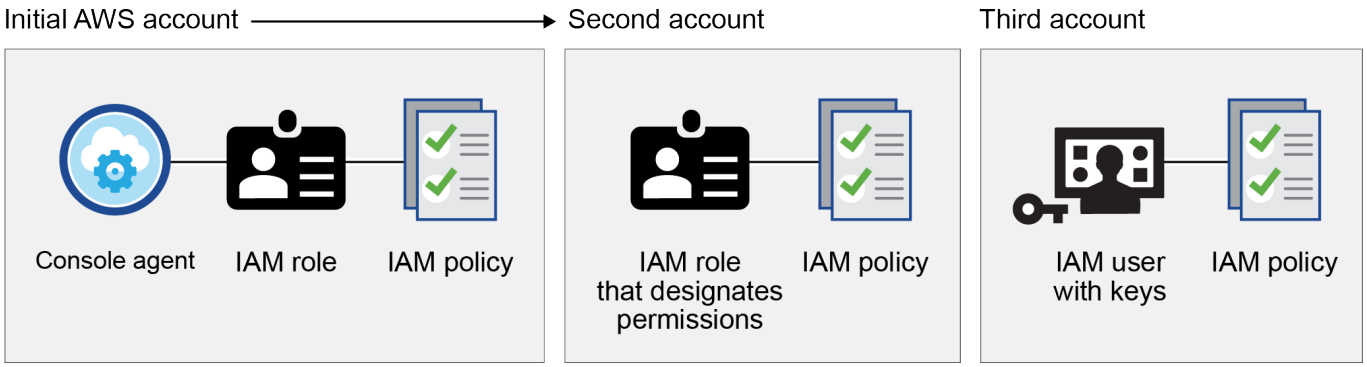
Puede agregar credenciales de AWS adicionales a la consola en los siguientes casos:

- Para usar su agente de consola existente con una cuenta de AWS adicional
- Para crear un nuevo agente en una cuenta de AWS específica
- Para crear y administrar sistemas de archivos FSx para ONTAP

Revise las secciones a continuación para obtener más detalles.

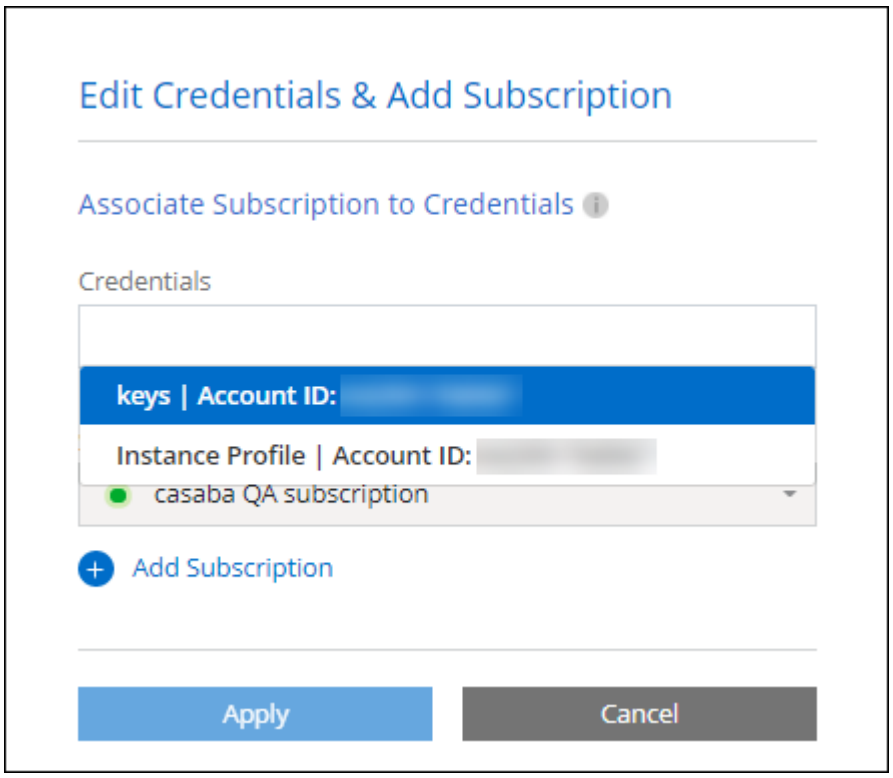
Agregue credenciales de AWS para usar un agente de consola con otra cuenta de AWS

Para utilizar la consola con cuentas de AWS adicionales, proporcione claves de AWS o el ARN de un rol en una cuenta de confianza. La siguiente imagen muestra dos cuentas adicionales, una que proporciona permisos a través de un rol de IAM en una cuenta confiable y otra a través de las claves de AWS de un usuario de IAM:



Para agregar las credenciales de la cuenta a la consola, especifique el nombre de recurso de Amazon (ARN) del rol de IAM o las claves de AWS para el usuario de IAM.

Por ejemplo, puede cambiar entre credenciales al crear un nuevo sistema Cloud Volumes ONTAP :



"Aprenda cómo agregar credenciales de AWS a un agente existente."

Agregue credenciales de AWS para crear un agente de consola

Agregar las credenciales de AWS otorga permisos para crear un agente de consola.

"Aprenda a agregar credenciales de AWS a la consola para crear un agente de consola"

Agregue credenciales de AWS para FSx para ONTAP

Agregue credenciales de AWS a la consola para proporcionar los permisos necesarios para crear y administrar un sistema FSx para ONTAP .

"Aprenda a agregar credenciales de AWS a la consola para Amazon FSx para ONTAP"

Credenciales y suscripciones al mercado

Debe asociar las credenciales que agregue a un agente de la consola con una suscripción a AWS Marketplace para pagar por Cloud Volumes ONTAP a una tarifa por hora (PAYGO) y otros servicios de datos de NetApp o mediante un contrato anual. "Aprenda a asociar una suscripción de AWS".

Tenga en cuenta lo siguiente sobre las credenciales de AWS y las suscripciones al mercado:

- Solo puede asociar una suscripción de AWS Marketplace con un conjunto de credenciales de AWS
- Puede reemplazar una suscripción de mercado existente con una nueva suscripción

Preguntas frecuentes

Las siguientes preguntas están relacionadas con credenciales y suscripciones.

¿Cómo puedo rotar de forma segura mis credenciales de AWS?

Como se describe en las secciones anteriores, la consola le permite proporcionar credenciales de AWS de varias maneras: un rol de IAM asociado con el agente de la consola, asumiendo un rol de IAM en una cuenta confiable o proporcionando claves de acceso de AWS.

Con las dos primeras opciones, la consola utiliza el servicio de token de seguridad de AWS para obtener credenciales temporales que rotan constantemente. Este proceso es la mejor práctica: es automático y seguro.

Si proporciona a la consola claves de acceso de AWS, debe rotar las claves actualizándolas en la consola a intervalos regulares. Este es un proceso completamente manual.

¿Puedo cambiar la suscripción de AWS Marketplace para los sistemas Cloud Volumes ONTAP ?

Sí, puedes. Cuando cambia la suscripción de AWS Marketplace asociada a un conjunto de credenciales, todos los sistemas Cloud Volumes ONTAP existentes y nuevos se cargan a la nueva suscripción.

"Aprenda a asociar una suscripción de AWS" .

¿Puedo agregar varias credenciales de AWS, cada una con diferentes suscripciones al mercado?

Todas las credenciales de AWS que pertenecen a la misma cuenta de AWS se asociarán con la misma suscripción de AWS Marketplace.

Si tiene varias credenciales de AWS que pertenecen a diferentes cuentas de AWS, esas credenciales se pueden asociar con la misma suscripción de AWS Marketplace o con diferentes suscripciones.

¿Puedo mover sistemas Cloud Volumes ONTAP existentes a una cuenta de AWS diferente?

No, no es posible mover los recursos de AWS asociados con su sistema Cloud Volumes ONTAP a una cuenta de AWS diferente.

¿Cómo funcionan las credenciales para las implementaciones del mercado y las implementaciones locales?

Las secciones anteriores describen el método de implementación recomendado para el agente de la consola, que es desde la consola. También puede implementar un agente en AWS desde AWS Marketplace y puede instalar manualmente el software del agente de consola en su propio host Linux o en su VCenter.

Si utiliza el Marketplace, los permisos se proporcionan de la misma manera. Solo necesita crear y configurar manualmente el rol de IAM y luego proporcionar permisos para cualquier cuenta adicional.

Para las implementaciones locales, no puede configurar una función de IAM para la consola, pero puede proporcionar permisos mediante claves de acceso de AWS.

Para saber cómo configurar permisos, consulte las siguientes páginas:

- Modo estándar
  - "Configurar permisos para una implementación de AWS Marketplace"

    - "Configurar permisos para implementaciones locales"
- Modo restringido
    - "Configurar permisos para el modo restringido"

Administrar las credenciales de AWS y las suscripciones al Marketplace para la NetApp Console

Agregue y administre las credenciales de AWS para poder implementar y administrar recursos de la nube en sus cuentas de AWS desde la NetApp Console. Si administra varias suscripciones de AWS Marketplace, puede asignar a cada una de ellas diferentes credenciales de AWS desde la página Credenciales.

Descripción general

Puede agregar credenciales de AWS a un agente de consola existente o directamente a la consola:

- Agregar credenciales de AWS adicionales a un agente existente

  Agregue credenciales de AWS a un agente de consola para administrar recursos en la nube. Aprenda a agregar credenciales de AWS a un agente de consola .

- Agregue credenciales de AWS a la consola para crear un agente de consola

  Agregar nuevas credenciales de AWS a la consola proporciona los permisos necesarios para crear un agente de consola. Aprenda a agregar credenciales de AWS a la NetApp Console .

- Agregue credenciales de AWS a la consola para FSx para ONTAP

  Agregue nuevas credenciales de AWS a la consola para crear y administrar FSx para ONTAP. "Aprenda a configurar permisos para FSx para ONTAP"

Cómo rotar credenciales

La NetApp Console le permite proporcionar credenciales de AWS de varias maneras: un rol de IAM asociado con la instancia del agente, asumiendo un rol de IAM en una cuenta confiable o proporcionando claves de acceso de AWS. "Obtenga más información sobre las credenciales y permisos de AWS" .

Con las dos primeras opciones, la consola utiliza el servicio de token de seguridad de AWS para obtener credenciales temporales que rotan constantemente. Este proceso es la mejor práctica porque es automático y seguro.

Rote manualmente las claves de acceso de AWS actualizándolas en la consola.

Agregar credenciales adicionales a un agente de consola

Agregue credenciales de AWS adicionales a un agente de consola para que tenga los permisos necesarios para administrar recursos y procesos dentro de su entorno de nube pública. Puede proporcionar el ARN de una función de IAM en otra cuenta o proporcionar claves de acceso de AWS.

"Descubra cómo la NetApp Console utiliza las credenciales y los permisos de AWS".

Conceder permisos

Otorgue permisos antes de agregar credenciales de AWS a un agente de consola. Los permisos permiten que un agente de consola administre recursos y procesos dentro de esa cuenta de AWS. Puede proporcionar los permisos con el ARN de un rol en una cuenta confiable o claves de AWS.

Si implementó un agente de consola desde la consola, se agregaron automáticamente las credenciales de AWS para la cuenta en la que implementó un agente de consola. Esto garantiza que se cuente con los permisos necesarios para administrar los recursos.

Opciones

- Otorgar permisos asumiendo un rol de IAM en otra cuenta
- Otorgar permisos proporcionando claves de AWS

Otorgar permisos asumiendo un rol de IAM en otra cuenta

Puede configurar una relación de confianza entre la cuenta de AWS de origen en la que implementó un agente de consola y otras cuentas de AWS mediante roles de IAM. Luego deberá proporcionar a la consola el ARN de los roles de IAM de las cuentas de confianza.

Si hay un agente de consola instalado localmente, no podrá utilizar este método de autenticación. Debes utilizar claves de AWS.

Pasos

1. Vaya a la consola de IAM en la cuenta de destino en la que desea proporcionar permisos a un agente de consola.
2. En Administración de acceso, seleccione **Roles > Crear rol** y siga los pasos para crear el rol.

   Asegúrese de hacer lo siguiente:

   - En **Tipo de entidad confiable**, seleccione **Cuenta AWS**.
   - Seleccione **Otra cuenta de AWS** e ingrese el ID de la cuenta donde reside una instancia del agente de consola.
   - Cree las políticas necesarias copiando y pegando el contenido de"Las políticas de IAM para un agente de consola" .
3. Copia el ARN del rol de IAM para que puedas pegarlo en la consola más adelante.

Resultado

La cuenta tiene los permisos requeridos. Ahora puedes agregar las credenciales a un agente de consola .

Otorgar permisos proporcionando claves de AWS

Si desea proporcionar a la consola claves de AWS para un usuario de IAM, deberá otorgarle los permisos necesarios a ese usuario. La política de IAM de la consola define las acciones y los recursos de AWS que la consola puede utilizar.

Debe utilizar este método de autenticación si hay un agente de consola instalado localmente. No puedes utilizar un rol IAM.

Pasos

1. Desde la consola de IAM, cree políticas copiando y pegando el contenido de"Las políticas de IAM para un agente de consola" .

   "Documentación de AWS: Creación de políticas de IAM"

2. Adjunte las políticas a un rol de IAM o a un usuario de IAM.
   - "Documentación de AWS: Creación de roles de IAM"
   - "Documentación de AWS: Cómo agregar y eliminar políticas de IAM"

Agregar las credenciales a un agente existente

Después de proporcionar una cuenta de AWS con los permisos necesarios, puede agregar las credenciales para esa cuenta a un agente existente. Esto le permite iniciar sistemas Cloud Volumes ONTAP en esa cuenta utilizando el mismo agente.

> Las nuevas credenciales de su proveedor de nube pueden tardar unos minutos en estar disponibles.

Pasos

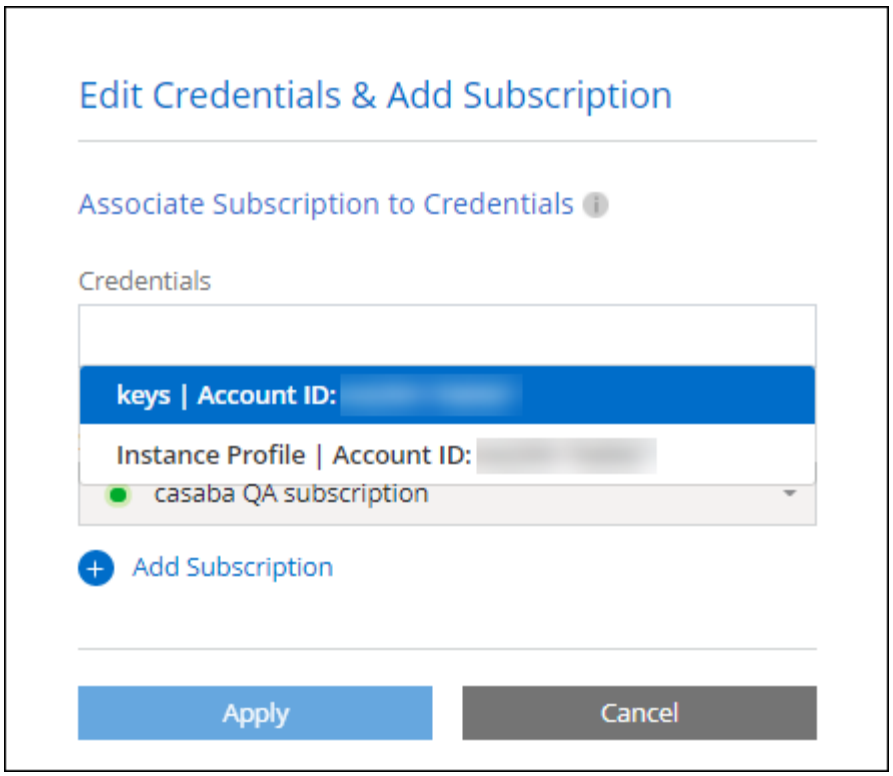
1. Utilice la barra de navegación superior para seleccionar un agente de consola al que desea agregar credenciales.
2. En la barra de navegación izquierda, seleccione **Administración > Credenciales**.
3. En la página **Credenciales de la organización**, seleccione **Agregar credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: seleccione **Amazon Web Services > Agente**.
   b. **Definir credenciales**: proporcione el ARN (nombre de recurso de Amazon) de una función de IAM confiable o ingrese una clave de acceso y una clave secreta de AWS.
   c. **Suscripción al Marketplace**: asocie una suscripción al Marketplace con estas credenciales suscribiéndose ahora o seleccionando una suscripción existente.

      Para pagar servicios a una tarifa por hora (PAYGO) o con un contrato anual, debe asociar las credenciales de AWS con su suscripción a AWS Marketplace.

   d. **Revisar**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Resultado

Ahora puede cambiar a un conjunto diferente de credenciales desde la página Detalles y credenciales al agregar una suscripción a la Consola.



Agregar credenciales a la consola para crear un agente de consola

Agregue credenciales de AWS proporcionando el ARN de una función de IAM que otorga los permisos necesarios para crear un agente de consola. Puede elegir estas credenciales al crear un nuevo agente.

Configurar la función IAM

Configure una función de IAM que permita que la capa de software como servicio (SaaS) de la NetApp Console asuma la función.

Pasos

1. Vaya a la consola IAM en la cuenta de destino.
2. En Administración de acceso, seleccione **Roles > Crear rol** y siga los pasos para crear el rol.

   Asegúrese de hacer lo siguiente:

   - En **Tipo de entidad confiable**, seleccione **Cuenta AWS**.
   - Seleccione **Otra cuenta de AWS** e ingrese el ID de la NetApp Console : 952013314444
   - Específicamente para Amazon FSx for NetApp ONTAP , edite la política **Relaciones de confianza** para incluir "AWS": "arn:aws:iam::952013314444:root".

     Por ejemplo, la política debería verse así:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
Referirse a "Documentación de AWS Identity and Access Management (IAM)" para obtener más información sobre el acceso a recursos entre cuentas en IAM.

- Cree una política que incluya los permisos necesarios para crear un agente de consola.
  - "Ver los permisos necesarios para FSx para ONTAP"
  - "Ver la política de implementación del agente"

3. Copia el ARN del rol de IAM para que puedas pegarlo en la consola en el siguiente paso.

Resultado

El rol IAM ahora tiene los permisos necesarios. Ahora puedes agregarlo a la consola.

Añade las credenciales

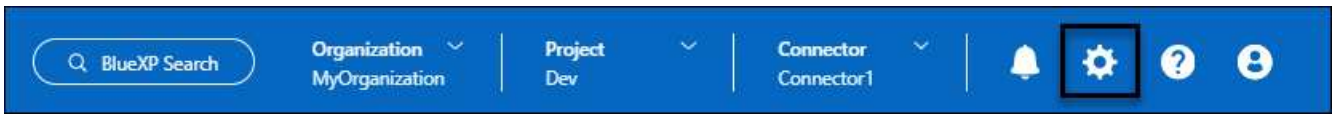
Después de proporcionar al rol IAM los permisos necesarios, agregue el ARN del rol a la consola.

Antes de empezar

Si acaba de crear el rol de IAM, es posible que pasen algunos minutos hasta que esté disponible para su uso. Espere unos minutos antes de agregar las credenciales a la consola.

Pasos

1. Seleccione **Administración > Credenciales**.



2. En la página **Credenciales de la organización**, seleccione **Agregar credenciales** y siga los pasos del asistente.
   a. **Ubicación de credenciales**: seleccione **Amazon Web Services > Consola**.
   b. **Definir credenciales**: proporcione el ARN (nombre de recurso de Amazon) de la función de IAM.
   c. **Revisar**: Confirme los detalles sobre las nuevas credenciales y seleccione **Agregar**.

Agregar credenciales a la consola para Amazon FSx para ONTAP

Para obtener más detalles, consulte la "La documentación de la consola para Amazon FSx para ONTAP"

Configurar una suscripción a AWS

Después de agregar sus credenciales de AWS, puede configurar una suscripción a AWS Marketplace con esas credenciales. La suscripción le permite pagar los servicios de datos de NetApp y Cloud Volumes ONTAP a una tarifa por hora (PAYGO) o mediante un contrato anual.

Hay dos escenarios en los que podrías configurar una suscripción a AWS Marketplace después de haber agregado las credenciales:

- No configuró una suscripción cuando agregó las credenciales inicialmente.
- Desea cambiar la suscripción de AWS Marketplace que está configurada con las credenciales de AWS.

  Reemplazar la suscripción actual del mercado por una nueva suscripción cambia la suscripción del mercado para cualquier sistema Cloud Volumes ONTAP existente y todos los sistemas nuevos.

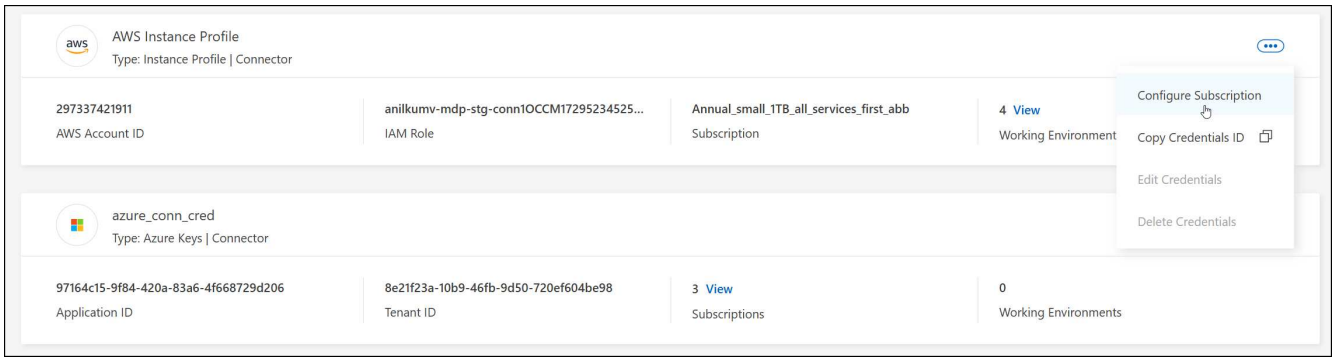
Antes de empezar

Debe crear un agente de consola antes de poder configurar una suscripción. "Aprenda a crear un agente de consola" .

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**.

Asociar una suscripción existente con su organización

Cuando se suscribe desde AWS Marketplace, el último paso del proceso es asociar la suscripción con su organización. Si no completó este paso, no podrá utilizar la suscripción con su organización.

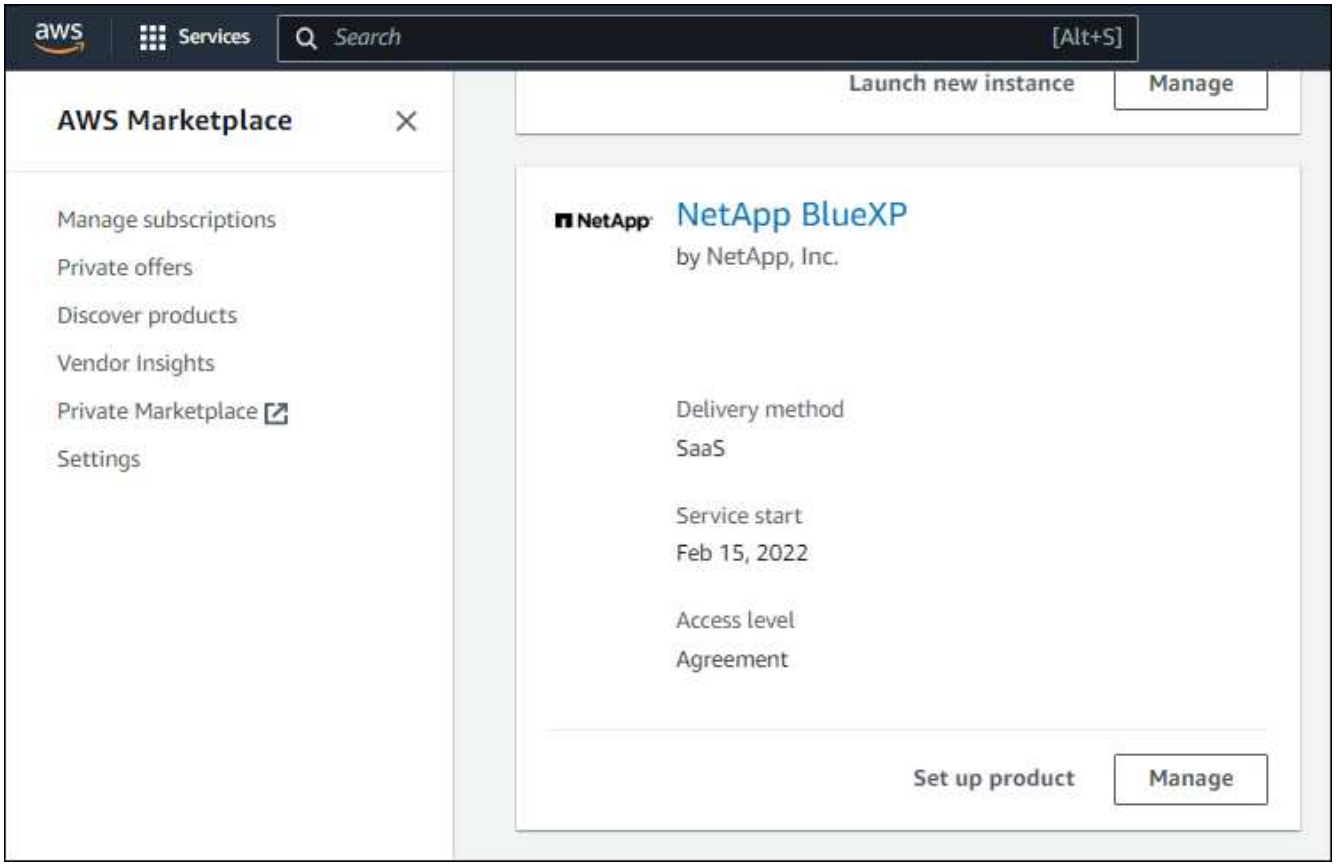
- "Obtenga más información sobre los modos de implementación de la consola"
- "Obtenga más información sobre la gestión de identidad y acceso de la consola"

Siga los pasos a continuación si se suscribió a NetApp Intelligent Services desde AWS Marketplace, pero omitió el paso para asociar la suscripción con su cuenta.

Pasos

1. Confirme que no asoció su suscripción con su organización de la consola.
   a. Desde el menú de navegación, seleccione **Administración > Licenses and subscriptions**.
   b. Seleccione **Suscripciones**.
   c. Verifica que tu suscripción no aparezca.

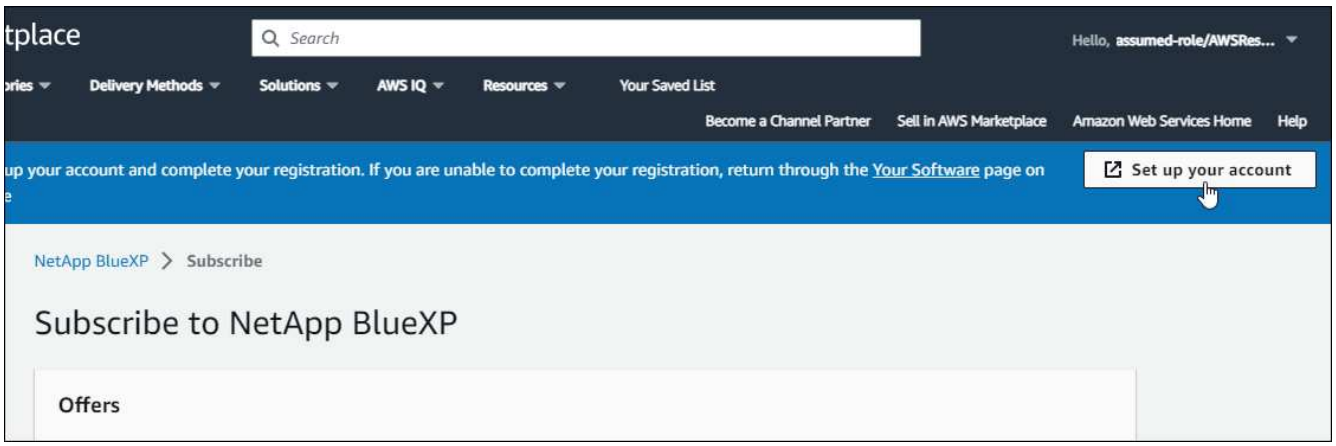
      Solo verás las suscripciones asociadas con la organización o cuenta que estás viendo actualmente. Si no ve su suscripción, continúe con los siguientes pasos.
2. Inicie sesión en la consola de AWS y navegue a **Suscripciones de AWS Marketplace**.
3. Encuentra la suscripción.



4. Seleccione **Configurar producto**.

   La página de oferta de suscripción debería cargarse en una nueva pestaña o ventana del navegador.

5. Seleccione **Configurar su cuenta**.



   La página **Asignación de suscripción** en netapp.com debería cargarse en una nueva pestaña o ventana del navegador.

   Tenga en cuenta que es posible que se le solicite que inicie sesión en la consola primero.

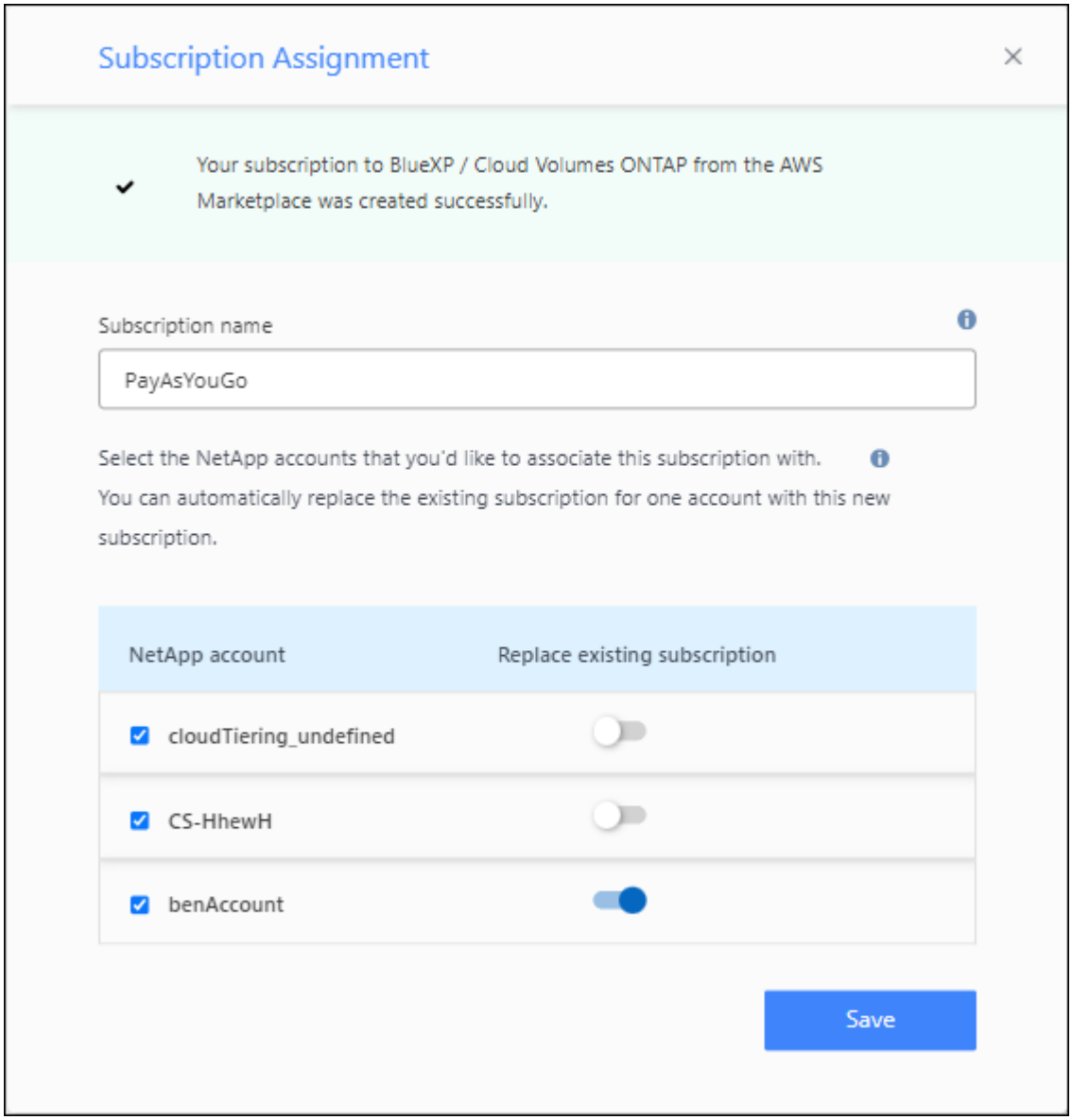
6. Desde la página **Asignación de suscripción**:

   - 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.

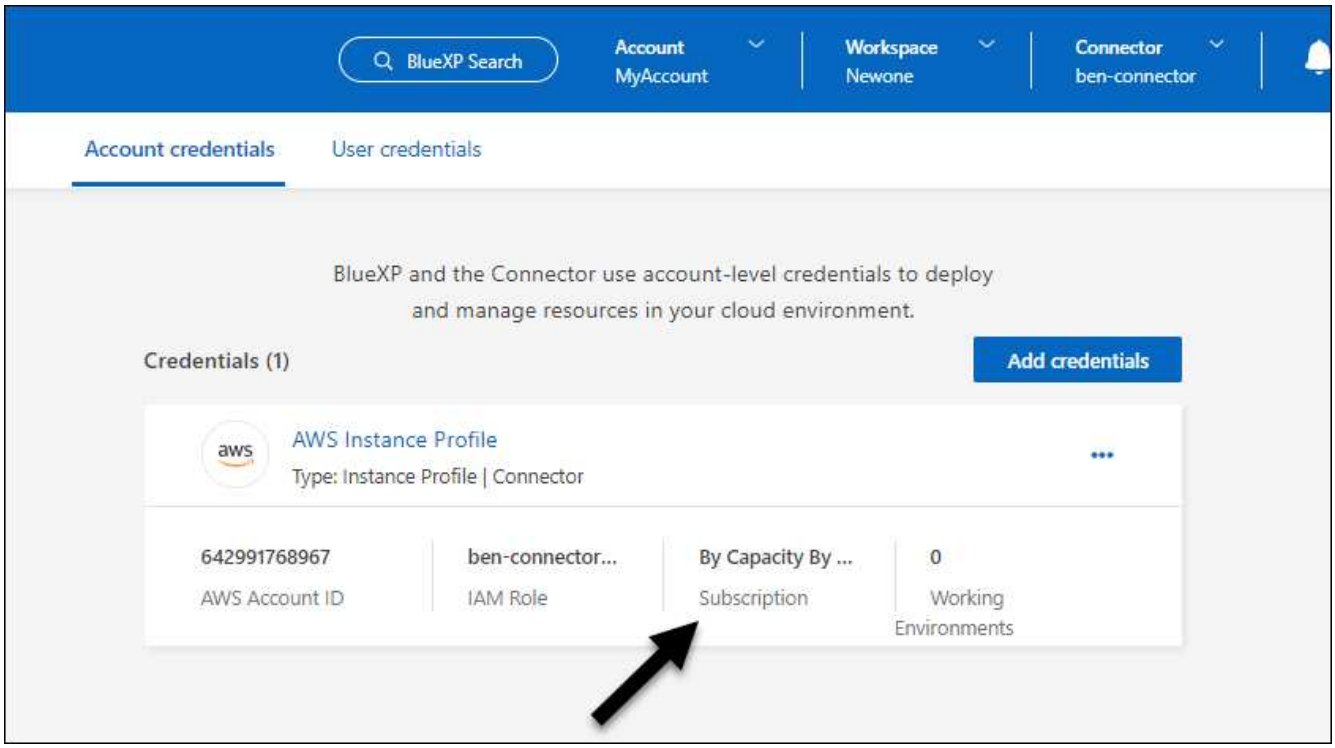
  Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.



7. Confirme que la suscripción esté asociada a su organización.
   a. Desde el menú de navegación, seleccione **Administración > Licencias y suscripciones**.
   b. Seleccione **Suscripciones**.
   c. Verifica que aparezca tu suscripción.
8. Confirme que la suscripción esté asociada con sus credenciales de AWS.
   a. Seleccione **Administración > Credenciales**.

b. En la página **Credenciales de la organización**, verifique que la suscripción esté asociada con sus credenciales de AWS.

   He aquí un ejemplo.



Editar credenciales

Edite sus credenciales de AWS cambiando el tipo de cuenta (claves de AWS o asumir rol), editando el nombre o actualizando las credenciales en sí (las claves o el ARN del rol).

> No puede editar las credenciales de un perfil de instancia que esté asociado con una instancia de agente de consola o una instancia de Amazon FSx para ONTAP . Solo puede cambiar el nombre de las credenciales de una instancia de FSx para ONTAP .

Pasos

1. Seleccione **Administración > Credenciales**.
2. En la página **Credenciales de la organización**, seleccione el menú de acciones para un conjunto de credenciales y luego seleccione **Editar credenciales**.
3. Realice los cambios necesarios y luego seleccione **Aplicar**.

Eliminar credenciales

Si ya no necesita un conjunto de credenciales, puede eliminarlas. Solo puedes eliminar credenciales que no estén asociadas a un sistema.

> No se pueden eliminar las credenciales de un perfil de instancia que esté asociado con un agente de consola.

Pasos

1. Seleccione **Administración > Credenciales**.
2. En la página **Credenciales de la organización** o **Credenciales de la cuenta**, seleccione el menú de acciones para un conjunto de credenciales y luego seleccione **Eliminar credenciales**.
3. Seleccione **Eliminar** para confirmar.

Azur

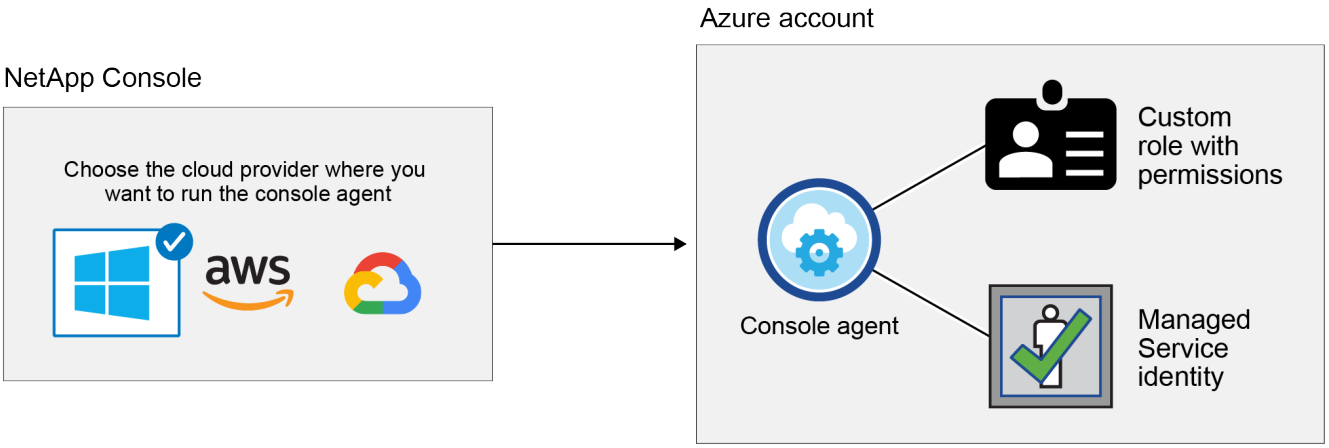
Obtenga información sobre las credenciales y los permisos de Azure en la NetApp Console

Descubra cómo la NetApp Console usa las credenciales de Azure para realizar acciones en su nombre y cómo esas credenciales se asocian con las suscripciones del Marketplace. Comprender estos detalles puede resultar útil al administrar las credenciales de una o más suscripciones de Azure. Por ejemplo, es posible que desee saber cuándo agregar credenciales de Azure adicionales a la consola.

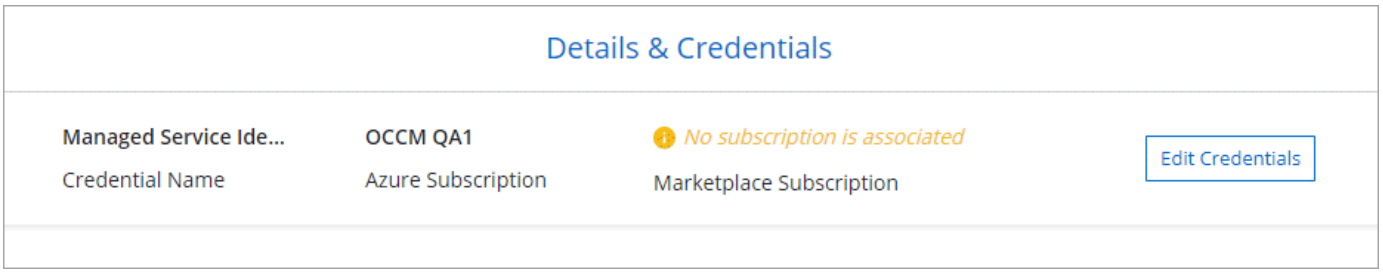
Credenciales iniciales de Azure

Al implementar un agente de consola desde la consola, debe usar una cuenta de Azure o una entidad de servicio que tenga permisos para implementar la máquina virtual del agente de consola. Los permisos necesarios se enumeran en el"Política de implementación de agentes para Azure" .

Cuando la consola implementa la máquina virtual del agente de consola en Azure, habilita una "identidad administrada asignada por el sistema" en la máquina virtual, crea un rol personalizado y lo asigna a la máquina virtual. El rol proporciona a la consola los permisos necesarios para administrar recursos y procesos dentro de esa suscripción de Azure. "Revisar cómo la Consola utiliza los permisos" .



Si crea un nuevo sistema para Cloud Volumes ONTAP, la consola selecciona estas credenciales de Azure de forma predeterminada:



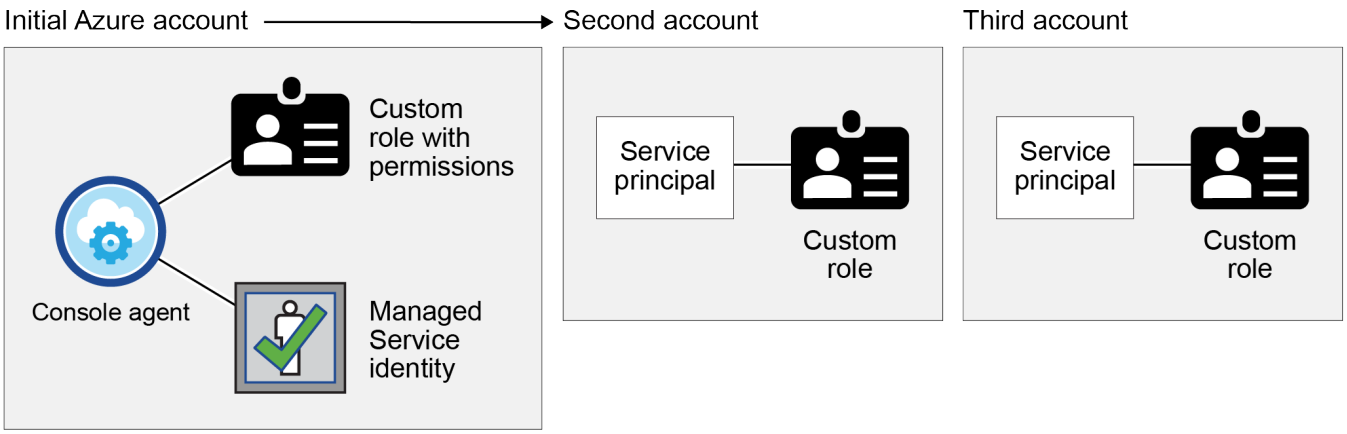
Puede implementar todos sus sistemas Cloud Volumes ONTAP utilizando las credenciales iniciales de Azure o puede agregar credenciales adicionales.

Suscripciones adicionales de Azure para una identidad administrada

La identidad administrada asignada por el sistema asignada a la máquina virtual del agente de consola está asociada con la suscripción en la que inició el agente de consola. Si desea seleccionar una suscripción de Azure diferente, deberá:"asociar la identidad administrada con esas suscripciones" .

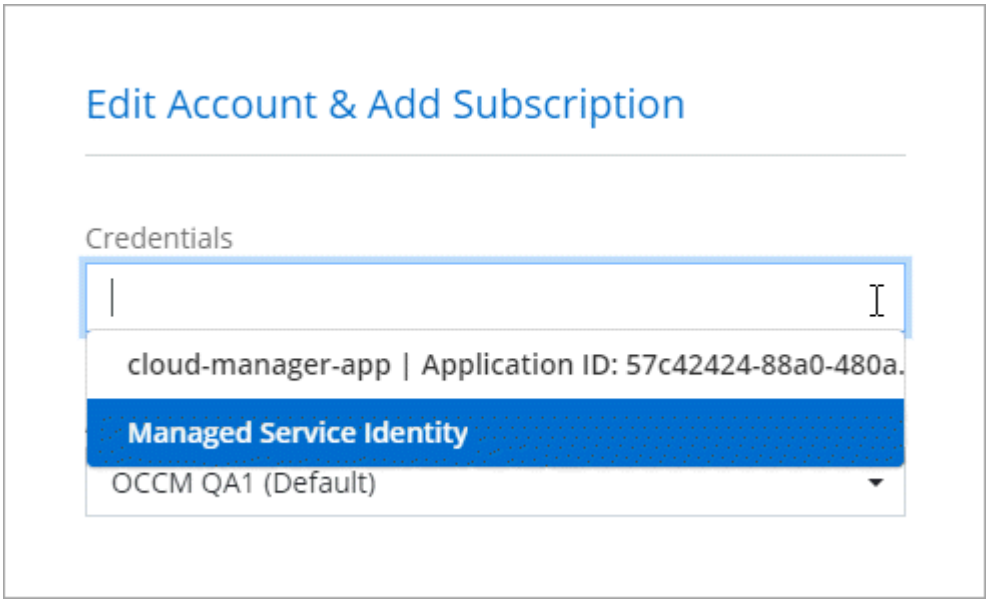
Credenciales adicionales de Azure

Si desea utilizar diferentes credenciales de Azure con la consola, debe otorgar los permisos necesarios mediante"Creación y configuración de una entidad de servicio en Microsoft Entra ID" para cada cuenta de Azure. La siguiente imagen muestra dos cuentas adicionales, cada una configurada con una entidad de servicio y un rol personalizado que proporciona permisos:



Entonces lo harías"Agregue las credenciales de la cuenta a la consola" proporcionando detalles sobre la entidad principal del servicio AD.

Por ejemplo, puede cambiar entre credenciales al crear un nuevo sistema Cloud Volumes ONTAP :



Credenciales y suscripciones al mercado

Las credenciales que agrega a un agente de consola deben estar asociadas a una suscripción de Azure Marketplace para que pueda pagar Cloud Volumes ONTAP a una tarifa por hora (PAYGO) o por los servicios de datos de NetApp o mediante un contrato anual.

"Aprenda a asociar una suscripción de Azure" .

Tenga en cuenta lo siguiente sobre las credenciales de Azure y las suscripciones al Marketplace:

- Solo puede asociar una suscripción de Azure Marketplace con un conjunto de credenciales de Azure
- Puede reemplazar una suscripción de mercado existente con una nueva suscripción

Preguntas frecuentes

La siguiente pregunta está relacionada con credenciales y suscripciones.

¿Puedo cambiar la suscripción de Azure Marketplace para los sistemas Cloud Volumes ONTAP ?

Sí, puedes. Cuando cambia la suscripción de Azure Marketplace asociada con un conjunto de credenciales de Azure, todos los sistemas Cloud Volumes ONTAP existentes y nuevos se cobrarán a la nueva suscripción.

"Aprenda a asociar una suscripción de Azure" .

¿Puedo agregar varias credenciales de Azure, cada una con diferentes suscripciones al Marketplace?

Todas las credenciales de Azure que pertenecen a la misma suscripción de Azure se asociarán con la misma suscripción de Azure Marketplace.

Si tiene varias credenciales de Azure que pertenecen a diferentes suscripciones de Azure, esas credenciales se pueden asociar con la misma suscripción de Azure Marketplace o con diferentes suscripciones de Marketplace.

¿Puedo mover sistemas Cloud Volumes ONTAP existentes a una suscripción de Azure diferente?

No, no es posible mover los recursos de Azure asociados con su sistema Cloud Volumes ONTAP a una suscripción de Azure diferente.

¿Cómo funcionan las credenciales para las implementaciones del mercado y las implementaciones locales?

Las secciones anteriores describen el método de implementación recomendado para el agente de la consola, que es desde la consola. También puede implementar un agente de consola en Azure desde Azure Marketplace y puede instalar el software del agente de consola en su propio host Linux.

Si usa Marketplace, puede proporcionar permisos asignando una función personalizada a la máquina virtual del agente de consola y a una identidad administrada asignada por el sistema, o puede usar una entidad de servicio de Microsoft Entra.

Para las implementaciones locales, no es posible configurar una identidad administrada para el agente de la consola, pero sí se pueden proporcionar permisos mediante una entidad de servicio.

Para saber cómo configurar permisos, consulte las siguientes páginas:

- Modo estándar

- "Configurar permisos para una implementación de Azure Marketplace"
- "Configurar permisos para implementaciones locales"

- Modo restringido
  - "Configurar permisos para el modo restringido"

Administrar credenciales de Azure y suscripciones de Marketplace para la NetApp Console

Agregue y administre las credenciales de Azure para que la NetApp Console tenga los permisos que necesita para implementar y administrar recursos en la nube en sus suscripciones de Azure. Si administra varias suscripciones de Azure Marketplace, puede asignar a cada una de ellas diferentes credenciales de Azure desde la página Credenciales.

Descripción general

Hay dos formas de agregar suscripciones y credenciales de Azure adicionales en la consola.

1. Asocie suscripciones adicionales de Azure con la identidad administrada de Azure.
2. Para implementar Cloud Volumes ONTAP con diferentes credenciales de Azure, otorgue permisos de Azure mediante una entidad de servicio y agregue sus credenciales a la consola.

Asociar suscripciones adicionales de Azure con una identidad administrada

La consola le permite elegir las credenciales de Azure y la suscripción de Azure en la que desea implementar Cloud Volumes ONTAP. No puede seleccionar una suscripción de Azure diferente para el perfil de identidad administrada a menos que asocie la "identidad administrada" con esas suscripciones.

Acerca de esta tarea

Una identidad administrada es"la cuenta inicial de Azure" cuando implementa un agente de consola desde la consola. Cuando se implementa el agente de consola, la consola asigna el rol de Operador de consola a la máquina virtual del agente de consola.

Pasos

1. Inicie sesión en el portal de Azure.
2. Abra el servicio **Suscripciones** y luego seleccione la suscripción en la que desea implementar Cloud Volumes ONTAP.
3. Seleccione **Control de acceso (IAM)**.
   a. Seleccione **Agregar** > **Agregar asignación de rol** y luego agregue los permisos:
      - Seleccione el rol de **Operador de consola**.

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

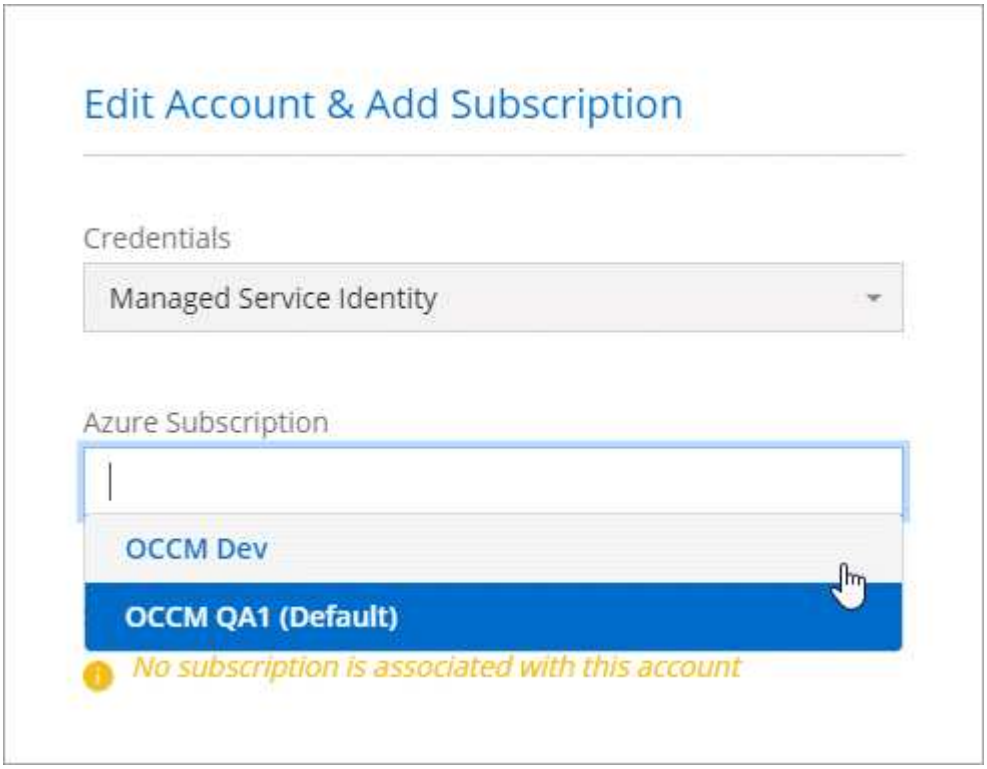
      - Asignar acceso a una **Máquina Virtual**.
      - Seleccione la suscripción en la que se creó una máquina virtual del agente de consola.
      - Seleccione una máquina virtual del agente de consola.

- Seleccione **Guardar**.

4. Repita estos pasos para suscripciones adicionales.

Resultado

Al crear un nuevo sistema, ahora puede seleccionar entre varias suscripciones de Azure para el perfil de identidad administrada.



Agregar credenciales de Azure adicionales a la NetApp Console

Cuando se implementa un agente de consola desde la consola, la consola habilita una identidad administrada asignada por el sistema en la máquina virtual que tiene los permisos necesarios. La consola selecciona estas credenciales de Azure de forma predeterminada cuando crea un nuevo sistema para Cloud Volumes ONTAP.

No se agrega un conjunto inicial de credenciales si instaló manualmente un software de agente de consola en un sistema existente. "Obtenga información sobre las credenciales y los permisos de Azure" .

Si desea implementar Cloud Volumes ONTAP con credenciales de Azure *diferentes*, debe otorgar los permisos necesarios creando y configurando una entidad de servicio en Microsoft Entra ID para cada cuenta de Azure. Luego puedes agregar las nuevas credenciales a la consola.

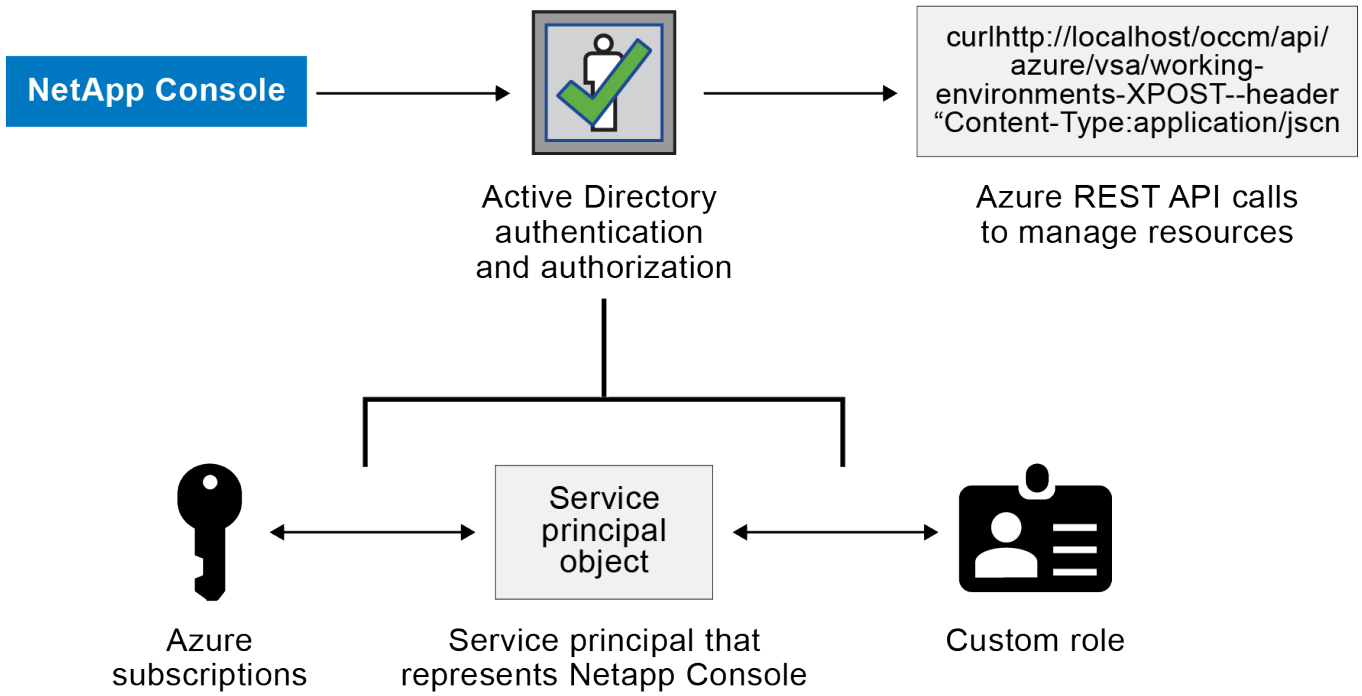
Otorgar permisos de Azure mediante una entidad de servicio

La consola necesita permisos para realizar acciones en Azure. Puede otorgar los permisos necesarios a una cuenta de Azure creando y configurando una entidad de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que necesita la consola.

Acerca de esta tarea

La siguiente imagen muestra cómo la consola obtiene permisos para realizar operaciones en Azure. Un objeto principal de servicio, que está vinculado a una o más suscripciones de Azure, representa la consola en

Microsoft Entra ID y se asigna a un rol personalizado que permite los permisos necesarios.



Pasos

1. Crear una aplicación Microsoft Entra .
2. Asignar la aplicación a un rol .
3. Agregar permisos de la API de administración de servicios de Windows Azure .
4. Obtener el ID de la aplicación y el ID del directorio .
5. Crear un secreto de cliente .

Crear una aplicación Microsoft Entra

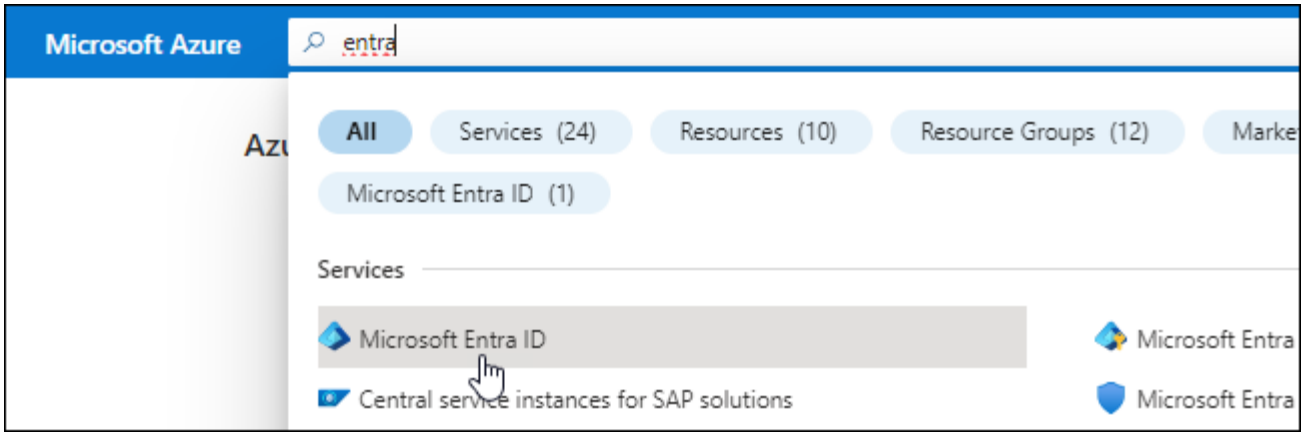
Cree una aplicación Microsoft Entra y una entidad de servicio que la consola pueda usar para el control de acceso basado en roles.

Pasos

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

Debe vincular la entidad de servicio a una o más suscripciones de Azure y asignarle el rol personalizado "Operador de consola" para que la consola tenga permisos en Azure.

Pasos

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 .

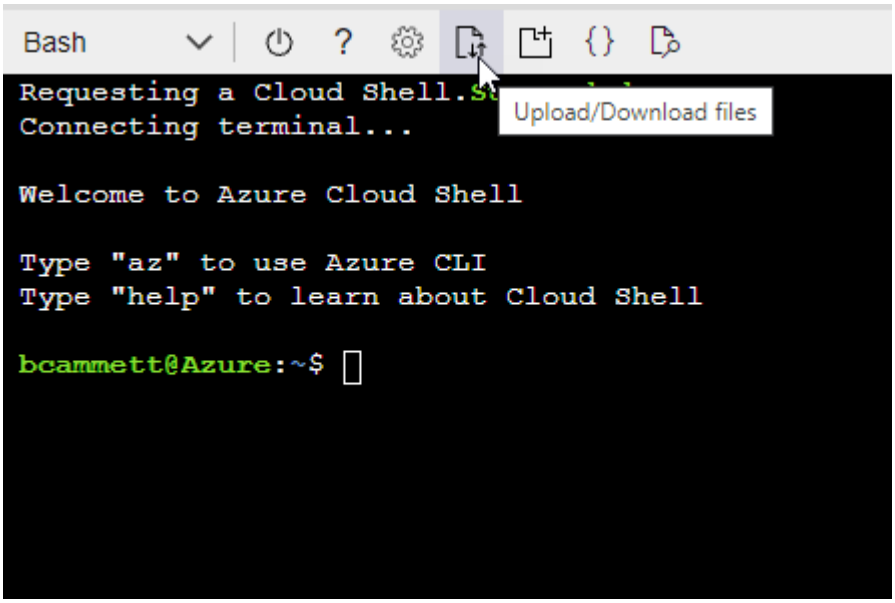
      Ejemplo

```
"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
```

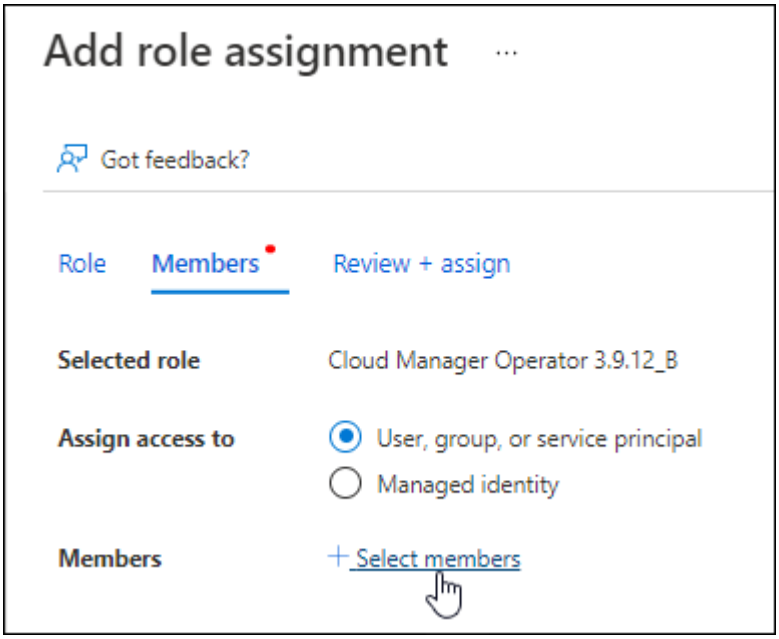
Ahora debería tener un rol personalizado llamado Operador de consola que puede asignar a la máquina virtual del agente de consola.

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:

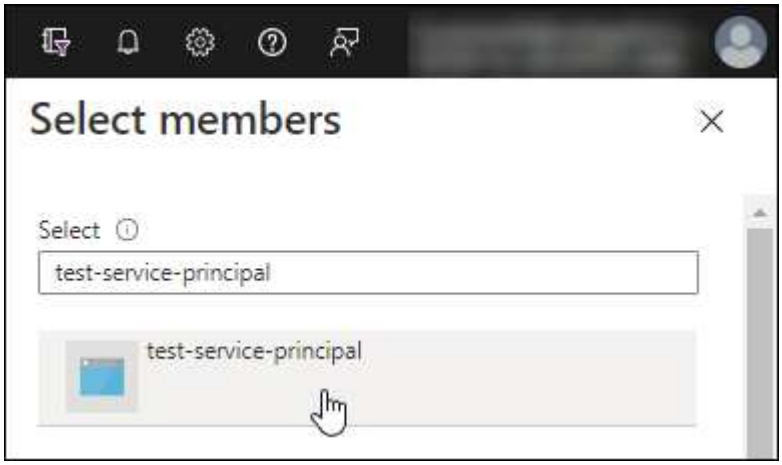
- Mantenga seleccionado **Usuario, grupo o entidad de servicio**.

- 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.

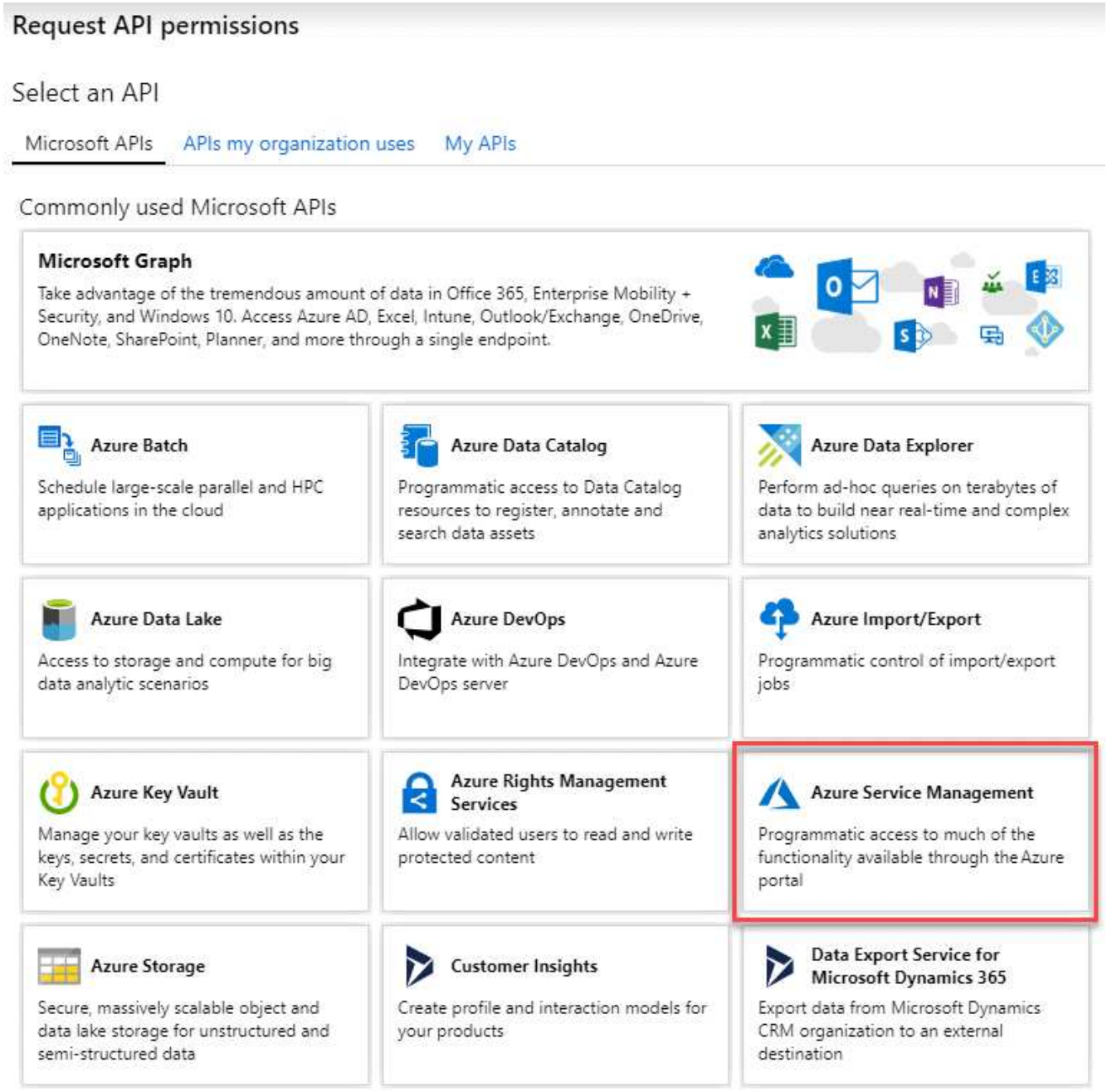
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones de Azure, debe vincular la entidad de servicio a cada una de esas suscripciones. En la NetApp Console, puede seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

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

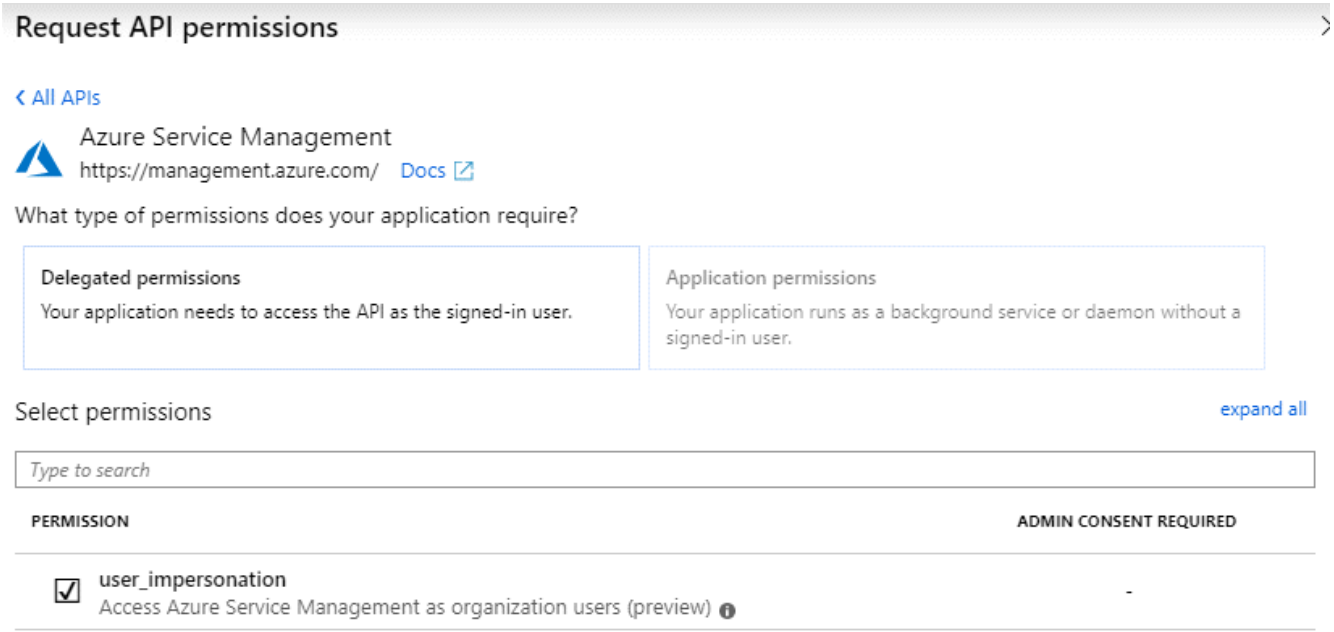
Debe asignar permisos de "API de administración de servicios de Windows Azure" a la entidad de servicio.

Pasos

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**.

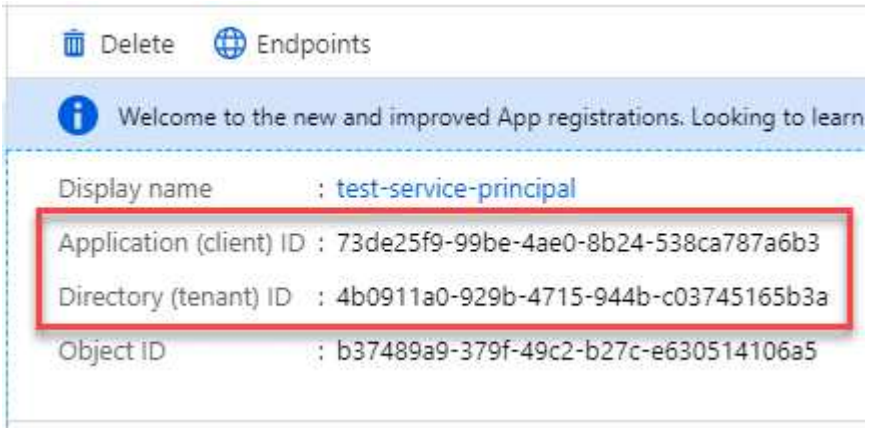


Obtener el ID de la aplicación y el ID del directorio

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.

Pasos

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

Cree un secreto de cliente y proporcione su valor a la consola para la autenticación con Microsoft Entra ID.

Pasos

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.

Añade las credenciales a la consola

Después de proporcionar una cuenta de Azure con los permisos necesarios, puede agregar las credenciales para esa cuenta a la consola. Al completar este paso podrá iniciar Cloud Volumes ONTAP con diferentes credenciales de Azure.

Antes de empezar

Si acaba de crear estas credenciales en su proveedor de nube, es posible que pasen algunos minutos hasta que estén disponibles para su uso. Espere unos minutos antes de agregar las credenciales a la consola.

Antes de empezar

Debe crear un agente de consola antes de poder cambiar la configuración de la consola. "Aprenda a crear un agente de consola" .

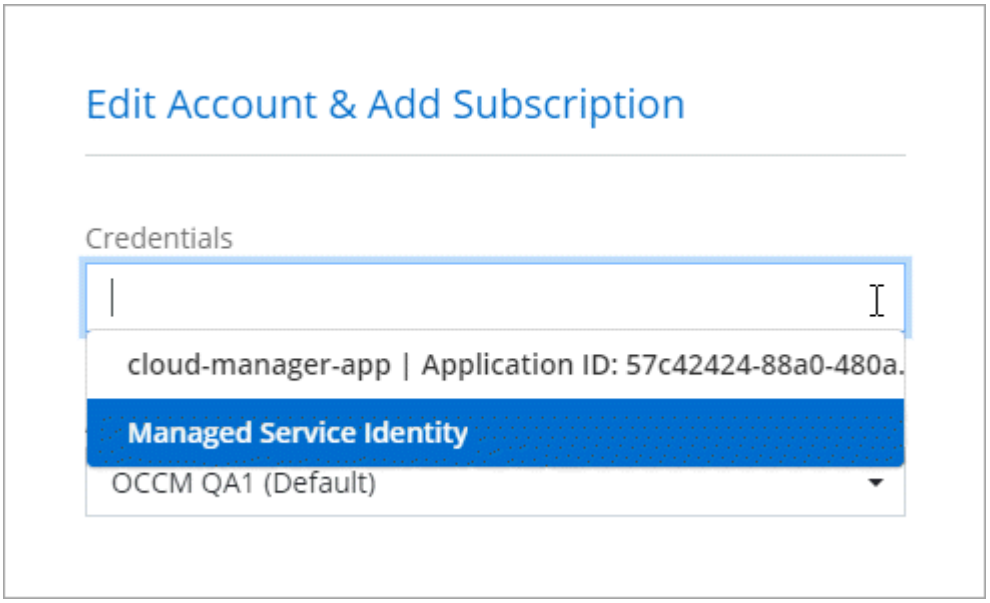
Pasos

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

Puede cambiar a un conjunto diferente de credenciales desde la página Detalles y Credenciales "al agregar un sistema a la consola"



Administrar credenciales existentes

Administre las credenciales de Azure que ya agregó a la consola asociando una suscripción de Marketplace, editando las credenciales y eliminándolas.

Asociar una suscripción de Azure Marketplace a las credenciales

Después de agregar sus credenciales de Azure a la consola, puede asociar una suscripción de Azure Marketplace a esas credenciales. Puede utilizar la suscripción para crear un sistema Cloud Volumes ONTAP de pago por uso y acceder a los servicios de datos de NetApp .

Hay dos escenarios en los que podría asociar una suscripción de Azure Marketplace después de haber agregado las credenciales a la consola:

- No asociaste una suscripción cuando agregaste inicialmente las credenciales a la consola.
- Desea cambiar la suscripción de Azure Marketplace que está asociada con las credenciales de Azure.

  Al reemplazar la suscripción actual del mercado, se actualiza para los sistemas Cloud Volumes ONTAP existentes y nuevos.

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**.

Editar credenciales

Edite sus credenciales de Azure en la consola. Por ejemplo, puede actualizar el secreto del cliente si se creó un nuevo secreto para la aplicación principal del servicio.

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Credenciales de la organización**.
3. Seleccione el menú de acciones para un conjunto de credenciales y luego seleccione **Editar credenciales**.
4. Realice los cambios necesarios y luego seleccione **Aplicar**.

Eliminar credenciales

Si ya no necesita un conjunto de credenciales, puede eliminarlas. Solo puedes eliminar credenciales que no estén asociadas a un sistema.

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Credenciales de la organización**.
3. En la página **Credenciales de la organización**, seleccione el menú de acciones para un conjunto de credenciales y luego seleccione **Eliminar credenciales**.
4. Seleccione **Eliminar** para confirmar.

Google Cloud

Obtenga más información sobre los proyectos y permisos de Google Cloud

Descubra cómo la NetApp Console utiliza las credenciales de Google Cloud para realizar acciones en su nombre y cómo esas credenciales se asocian con las suscripciones del mercado. Comprender estos detalles puede resultar útil al administrar las credenciales de uno o más proyectos de Google Cloud. Por ejemplo, es posible que desee obtener información sobre la cuenta de servicio asociada con la máquina virtual del agente de consola.

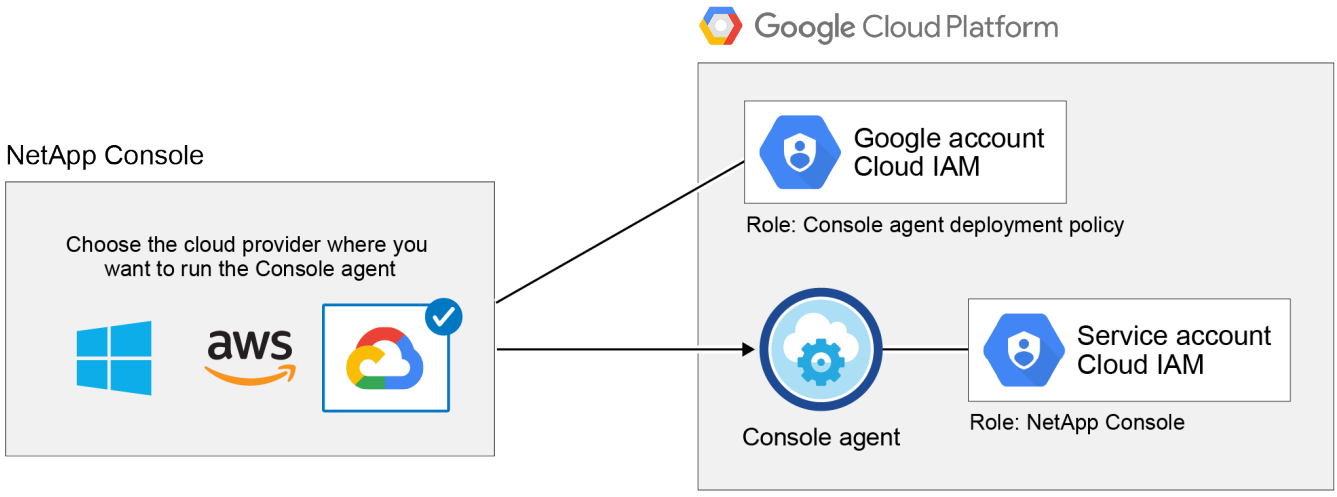
Proyecto y permisos para la NetApp Console

Antes de poder usar la consola para administrar recursos en su proyecto de Google Cloud, primero debe implementar un agente de consola. El agente no puede estar ejecutándose en sus instalaciones ni en un proveedor de nube diferente.

Se deben establecer dos conjuntos de permisos antes de implementar un agente de consola directamente desde la consola:

1. Debe implementar un agente de consola utilizando una cuenta de Google que tenga permisos para iniciar el agente de consola desde la consola.
2. Al implementar el agente de la consola, se le solicitará que seleccione un "cuenta de servicio" para el agente La consola obtiene permisos de la cuenta de servicio para crear y administrar sistemas Cloud Volumes ONTAP , administrar copias de seguridad mediante el respaldo y la recuperación de NetApp , y más. Los permisos se proporcionan adjuntando un rol personalizado a la cuenta de servicio.

La siguiente imagen representa los requisitos de permiso descritos en los números 1 y 2 anteriores:



Para saber cómo configurar permisos, consulte las siguientes páginas:

- "Configurar los permisos de Google Cloud para el modo estándar"
- "Configurar permisos para el modo restringido"

Credenciales y suscripciones al mercado

Cuando implementa un agente de consola en Google Cloud, la consola crea un conjunto predeterminado de credenciales para la cuenta de servicio de Google Cloud en el proyecto en el que reside el agente de consola. Estas credenciales deben estar asociadas a una suscripción a Google Cloud Marketplace para que pueda pagar los servicios de datos de Cloud Volumes ONTAP y NetApp .

"Aprenda a asociar una suscripción a Google Cloud Marketplace" .

Tenga en cuenta lo siguiente sobre las credenciales de Google Cloud y las suscripciones al mercado:

- Solo se puede asociar un conjunto de credenciales de Google Cloud con un agente de consola
- Solo puedes asociar una suscripción a Google Cloud Marketplace con las credenciales
- Puede reemplazar una suscripción de mercado existente con una nueva suscripción

Proyecto para Cloud Volumes ONTAP

Cloud Volumes ONTAP puede residir en el mismo proyecto que el agente de consola o en un proyecto diferente. Para implementar Cloud Volumes ONTAP en un proyecto diferente, primero debe agregar la cuenta de servicio y el rol del agente de consola a ese proyecto.

- "Aprenda a configurar la cuenta de servicio"
- "Aprenda a implementar Cloud Volumes ONTAP en Google Cloud y seleccione un proyecto"

Administrar los permisos del agente de la consola para las implementaciones de Google Cloud

Ocasionalmente, NetApp actualiza los permisos necesarios para la cuenta de servicio utilizada para el agente de consola cuando se implementa en Google Cloud.

"Verificar la lista de permisos de Google requeridos".

Utilice Google Cloud Console para actualizar la función de IAM asignada a la cuenta de servicio para que coincida con el nuevo conjunto de permisos.

"Documentación de Google Cloud: Editar una función personalizada"