Documentación de configuración y administración de la NetApp Console

NetApp Console setup and administration

NetApp
February 11, 2026

This PDF was generated from https://docs.netapp.com/es-es/console-setup-admin/index.html on February 11, 2026. Always check docs.netapp.com for the latest.

Tabla de contenidos

Documentación de configuración y administración de la NetApp Console . . . 1
Notas de la versión . . . 2
Qué hay de nuevo . . . 2
09 de febrero de 2026 . . . 2
13 de enero de 2026 . . . 2
10 de diciembre de 2025 . . . 3
10 de noviembre de 2025 . . . 4
6 de octubre de 2025 . . . 5
BlueXP ahora es NetApp Console . . . 5
Agente de consola 4.0.0 . . . 11
NetApp Console . . . 12
11 de agosto de 2025 . . . 13
31 de julio de 2025 . . . 14
21 de julio de 2025 . . . 14
14 de julio de 2025 . . . 15
9 de junio de 2025 . . . 16
29 de mayo de 2025 . . . 17
12 de mayo de 2025 . . . 17
14 de abril de 2025 . . . 19
28 de marzo de 2025 . . . 19
10 de marzo de 2025 . . . 20
6 de marzo de 2025 . . . 20
18 de febrero de 2025 . . . 21
10 de febrero de 2025 . . . 21
13 de enero de 2025 . . . 23
16 de diciembre de 2024 . . . 23
9 de diciembre de 2024 . . . 24
26 de noviembre de 2024 . . . 25
11 de noviembre de 2024 . . . 25
10 de octubre de 2024 . . . 26
7 de octubre de 2024 . . . 26
30 de septiembre de 2024 . . . 27
9 de septiembre de 2024 . . . 28
22 de agosto de 2024 . . . 30
8 de agosto de 2024 . . . 30
31 de julio de 2024 . . . 31
15 de julio de 2024 . . . 32
8 de julio de 2024 . . . 32
12 de junio de 2024 . . . 32
4 de junio de 2024 . . . 33
17 de mayo de 2024 . . . 34
Limitaciones conocidas de NetApp Console . . . 34
Limitaciones del agente de consola . . . 35

Empezar . . . 36
Aprenda los conceptos básicos . . . 36
Obtenga más información sobre la NetApp Console . . . 36
Obtenga más información sobre los modos de implementación de la NetApp Console . . . 39
Administrar las credenciales NSS asociadas con la NetApp Console . . . 46
Obtenga más información sobre los agentes de la NetApp Console . . . 50
Obtenga más información sobre la gestión de identidad y acceso de la NetApp Console . . . 54
Comience a usar NetApp Console (Saas) . . . 59
Flujo de trabajo de introducción (SaaS) . . . 59
Preparar el acceso a la red para la NetApp Console . . . 60
Regístrese o inicie sesión en la NetApp Console . . . 62
Comience a utilizar el asistente de la NetApp Console . . . 64
Introducción a NetApp Console (modo restringido) . . . 64
Flujo de trabajo de introducción (modo restringido) . . . 64
Prepárese para la implementación en modo restringido . . . 65
Implementar el agente de consola en modo restringido . . . 86
Suscribirse a NetApp Intelligent Services (modo restringido) . . . 98
Qué puedes hacer a continuación (modo restringido) . . . 104
Empieza con el modo privado . . . 104
Flujo de trabajo de introducción (modo privado de BlueXP) . . . 105
Utilice la NetApp Console . . . 107
Inicie sesión en la NetApp Console . . . 107
Trabajar con múltiples agentes de consola . . . 109
Cambiar entre agentes de la consola . . . 109
Ver métricas en la página de inicio de la NetApp Console . . . 110
Roles requeridos de la NetApp Console . . . 110
Habilitar que las métricas aparezcan en la página de inicio . . . 112
Ver la capacidad de almacenamiento general . . . 112
Ver alertas de ONTAP . . . 113
Ver la capacidad de rendimiento del almacenamiento . . . 114
Ver las licencias y suscripciones que tienes . . . 114
Ver el estado de resiliencia frente al ransomware . . . 115
Ver el estado de la copia de seguridad y recuperación . . . 115
Administrar la configuración de usuario de la NetApp Console . . . 115
Cambiar tu nombre para mostrar . . . 116
Mejora tu rol en modo de solo lectura . . . 116
Configurar la autenticación multifactor . . . 116
Regenera tu código de recuperación de MFA . . . 117
Eliminar su configuración de MFA . . . 117
Comuníquese con el administrador de su organización . . . 117
Configurar el modo oscuro (tema oscuro) . . . 118
Administrar y monitorear . . . 119
Asociar cuentas de soporte de NetApp . . . 119
Administrar las credenciales NSS asociadas con la NetApp Console . . . 119
Administrar las credenciales asociadas con el inicio de sesión de su NetApp Console . . . 122

Agentes de consola . . . 123
Obtenga más información sobre los agentes de la NetApp Console . . . 124
Implementar un agente de consola . . . 128
Mantener agentes de consola . . . 284
Administrar las credenciales del proveedor de la nube . . . 298
Gestión de identidad y acceso . . . 332
Obtenga más información sobre la gestión de identidad y acceso de la NetApp Console . . . 332
Comience a utilizar la identidad y el acceso en la NetApp Console . . . 336
Configurar la organización de su consola . . . 337
Agregue usuarios a su organización de la consola . . . 347
Gestionar el acceso y la seguridad de los usuarios . . . 350
Roles de acceso a la NetApp Console . . . 356
API de identidad y acceso . . . 377
Seguridad y cumplimiento . . . 379
Federación de identidades . . . 379
Aplicar permisos de ONTAP para la Vista avanzada de ONTAP (Administrador del sistema ONTAP) . . . 391
Habilitar el modo de solo lectura para una organización de NetApp Console . . . 392
Gestionar las asociaciones de la organización . . . 394
Asociaciones de organizaciones en NetApp Console . . . 394
Administrar asociaciones en la NetApp Console . . . 398
Administrar miembros para una organización asociada . . . 399
Proporcionar acceso a recursos a los usuarios asociados . . . 401
Trabajar en una organización asociada . . . 403
Supervisar las operaciones de la NetApp Console . . . 403
Auditar la actividad del usuario desde la página Auditoría . . . 403
Supervisar actividades mediante el Centro de notificaciones . . . 404
Referencia . . . 408
Consola de mantenimiento del agente . . . 408
Validación del agente con la consola de mantenimiento . . . 408
Comandos de proxy transparentes . . . 409
Permisos del agente del proveedor de nube y requisitos de red . . . 411
Resumen de permisos para la NetApp Console . . . 411
Permisos del agente de AWS y reglas de seguridad . . . 415
Permisos de Azure y reglas de seguridad requeridas . . . 448
Permisos de Google Cloud y reglas de firewall requeridas . . . 472
Acceso a la red requerido para 3.9.55 y anteriores . . . 495
Actualice su lista de puntos finales a la lista revisada para 4.0.0 y versiones superiores . . . 495
Puntos finales para la NetApp Console y los agentes de consola para la versión 3.9.55 y anteriores . . . 497
Puntos finales del proveedor de la nube contactados por el agente de la consola . . . 497
Puntos finales de servicios de datos contactados por el agente de la consola . . . 498
Requerir el uso de IMDSv2 en instancias de Amazon EC2 . . . 498
Configuración predeterminada para el agente de consola . . . 500
Configuración predeterminada con acceso a Internet . . . 500
Configuración predeterminada sin acceso a Internet . . . 501
Conocimiento y apoyo . . . 503

Regístrese para recibir asistencia . . . 503
Descripción general del registro de soporte . . . 503
Registrar la NetApp Console para obtener soporte de NetApp . . . 503
Asociar credenciales NSS para la compatibilidad con Cloud Volumes ONTAP . . . 505
Obtener ayuda . . . 507
Obtenga soporte para un servicio de archivos de un proveedor de nube . . . 507
Utilice opciones de autosuficiencia . . . 507
Cree un caso con el soporte de NetApp . . . 507
Gestione sus casos de soporte . . . 510
Avisos legales . . . 511
Copyright . . . 511
Marcas comerciales . . . 511
Patentes . . . 511
Política de privacidad . . . 511
Código abierto . . . 511

Documentación de configuración y administración de la NetApp Console

Notas de la versión

Qué hay de nuevo

Conozca las novedades en las funciones de administración de la NetApp Console : administración de identidad y acceso (IAM), agentes de consola, credenciales de proveedores de nube y más.

09 de febrero de 2026

Agente de Console 4.4.0

La versión 4.4.0 es compatible tanto con el modo estándar como con el modo restringido.

Esta versión del agente de la Console incluye mejoras de seguridad y correcciones de errores.

Administración de la NetApp Console

Esta versión incluye lo siguiente:

Soporte para el acceso basado en roles para NetApp Backup and Recovery workloads (Oracle y Microsoft SQL Server)

Puedes asociar cargas de trabajo de Backup and Recovery (Oracle y Microsoft SQL Server) con proyectos. Después de asignarlas a un proyecto, los usuarios que tengan asignado un rol de Backup and Recovery para el proyecto pueden trabajar con las cargas de trabajo. Otras cargas de trabajo no son compatibles con acceso basado en roles en este momento.

"Conoce más sobre cómo configurar el acceso basado en roles para las cargas de trabajo de Backup and Recovery."

13 de enero de 2026

Agente de consola 4.3.0

La versión 4.3.0 admite tanto el modo estándar como el modo restringido.

Esta versión del agente de consola incluye mejoras de seguridad, correcciones de errores y las siguientes características:

Capacidad para validar las conexiones de red de los agentes de la consola

Ahora puedes validar las conexiones de red de los agentes de Console conectados directamente desde la NetApp Console. Esta función te ayuda a verificar la conectividad y solucionar problemas con los agentes de Console. Esto se suma a la capacidad existente de ejecutar diagnósticos de red desde la línea de comandos de la consola de mantenimiento del agente de Console (CLI).

"Aprende cómo ejecutar la configuración desde NetApp Console."

Administración de la NetApp Console

Esta versión incluye lo siguiente:

Acceso basado en roles para grupos federados en la NetApp Console

NetApp Console admite la asignación de roles a grupos federados (por ejemplo, grupos de Active Directory), lo que permite a los administradores automatizar la incorporación y salida de usuarios en función de la membresía del grupo en el proveedor de identidad (IdP) de la organización. Esta función reduce la sobrecarga administrativa y garantiza un acceso seguro y consistente al actualizar instantáneamente el acceso a la consola a medida que cambian las membresías del grupo.

"Aprenda cómo proporcionar acceso a un grupo federado a su organización."

Compatibilidad con la federación cuando la NetApp Console está en modo restringido

Ahora puede habilitar la federación para una organización de NetApp Console que esté en modo restringido. Esto permite a los usuarios iniciar sesión en la consola utilizando sus credenciales corporativas mientras mantienen los beneficios de seguridad del modo restringido.

Modo de solo lectura

Puede configurar una organización de la NetApp Console en modo de solo lectura. En el modo de solo lectura, los usuarios pueden ver recursos y configuraciones, pero no pueden realizar cambios. Un administrador de organización o un superadministrador puede habilitar el modo de solo lectura para una organización. Cuando el modo de solo lectura está habilitado, los usuarios con roles administrativos deben elevar manualmente sus permisos para realizar cambios según sea necesario.

"Aprenda cómo habilitar el modo de solo lectura para una organización de consola."

"Aprenda cómo elevar su rol cuando su organización está en modo de solo lectura."

10 de diciembre de 2025

Agente de consola 4.2.0

La versión 4.2.0 admite tanto el modo estándar como el modo restringido.

Esta versión del agente de consola incluye mejoras de seguridad, correcciones de errores y las siguientes características:

Compatibilidad con Google Cloud Infrastructure Manager

NetApp ahora utiliza Google Cloud Infrastructure Manager (IM) en lugar de Google Cloud Deployment Manager para implementar agentes y administrarlos en Google Cloud. Este cambio se realizó porque Google dejará de usar"Administrador de implementación en la nube" .

- Cualquier agente nuevo 4.2.0 y superior usa Infrastructure Manager y debe actualizar los permisos de la cuenta de usuario y de la cuenta de servicio utilizados para la implementación."Ver el registro de cambios de permisos."
- Cuando implementa un agente, el sistema también crea un depósito de Google Cloud para almacenar archivos de implementación.

Comprobaciones de configuración mejoradas para los agentes de la consola

- El agente de consola ahora busca puntos finales obsoletos al realizar una verificación de configuración. Si no ha actualizado a la nueva lista de puntos finales para 4.0.0 o superior, las instalaciones tendrán éxito si el sistema puede acceder a la lista de puntos finales anterior."Obtenga más información sobre los puntos finales necesarios para los agentes de consola."
- Ejecute comprobaciones de configuración en los agentes de consola instalados desde la consola o la consola de mantenimiento del agente para verificar la conectividad y solucionar problemas."Aprenda a ejecutar comprobaciones de configuración en agentes de la consola."

Descargue directamente el software del agente desde la NetApp Console

Cuando necesite instalar manualmente un agente, puede acceder al software del agente directamente desde la NetApp Console , además del sitio de soporte de NetApp ."Aprenda cómo descargar el software del agente de la consola directamente desde la NetApp Console."

Administración de la NetApp Console

Esta versión incluye lo siguiente:

Capacidad de configurar notificaciones para credenciales que expiran

Establecer notificaciones para el vencimiento de credenciales en cuentas de servicio y federaciones. Elija entre siete o 30 días. La consola muestra notificaciones y envía correos electrónicos a los usuarios con el rol apropiado. Los administradores de la organización reciben notificaciones de la cuenta de servicio. Los administradores de la organización, los administradores de la federación y los espectadores de la federación reciben notificaciones de la federación.

Los inicios de sesión locales no están disponibles después de habilitar la federación

Después de activar la federación para una organización de la consola, los usuarios no pueden usar inicios de sesión locales y se les envía a inicios de sesión de federación.

Mejoras de usabilidad para las páginas de administración de almacenamiento

Ahora es más fácil ver y administrar información detallada sobre sus sistemas locales de ONTAP (y FSx para ONTAP) desde las páginas de administración de almacenamiento.

- La página * Discoverable systems* separa la información resumida de la visualización en pestañas de los sistemas disponibles, lo que facilita la visualización de información completa acerca de los sistemas detectables.

10 de noviembre de 2025

Agente de consola 4.1.0

Esta versión del agente de consola incluye mejoras de seguridad, correcciones de errores y las siguientes características:

La versión 4.1.0 está disponible para el modo estándar y el modo restringido.

Indicadores de estado del agente renombrados

Se renombraron los indicadores de estado del agente de la consola de **Activo** e **Inactivo** a **Conectado** y **Desconectado** para que su propósito sea más claro.

Compatibilidad con Red Hat Enterprise Linux (RHEL) 9.6 y Podman 5.4.0

Al instalar manualmente un agente de consola, el agente ahora admite RHEL 9.6 con Podman 5.4.0. Además, al usar RHEL 9 y versiones posteriores, NetApp admite podman-compose 1.5.0. "Ver requisitos del sistema operativo".

Administración de la NetApp Console

Esta versión incluye lo siguiente:

Nueva dirección de correo electrónico para las notificaciones de la NetApp Console

La dirección de correo electrónico que envía notificaciones de NetApp Console ha cambiado de **service@console.bluexp.netapp.com** a **service@console.bluexp.netapp.com**. NetApp recomienda

actualizar las reglas de correo electrónico para permitir **service@console.netapp.com** para garantizar que continúe recibiendo notificaciones por correo electrónico de la NetApp Console .

6 de octubre de 2025

BlueXP ahora es NetApp Console

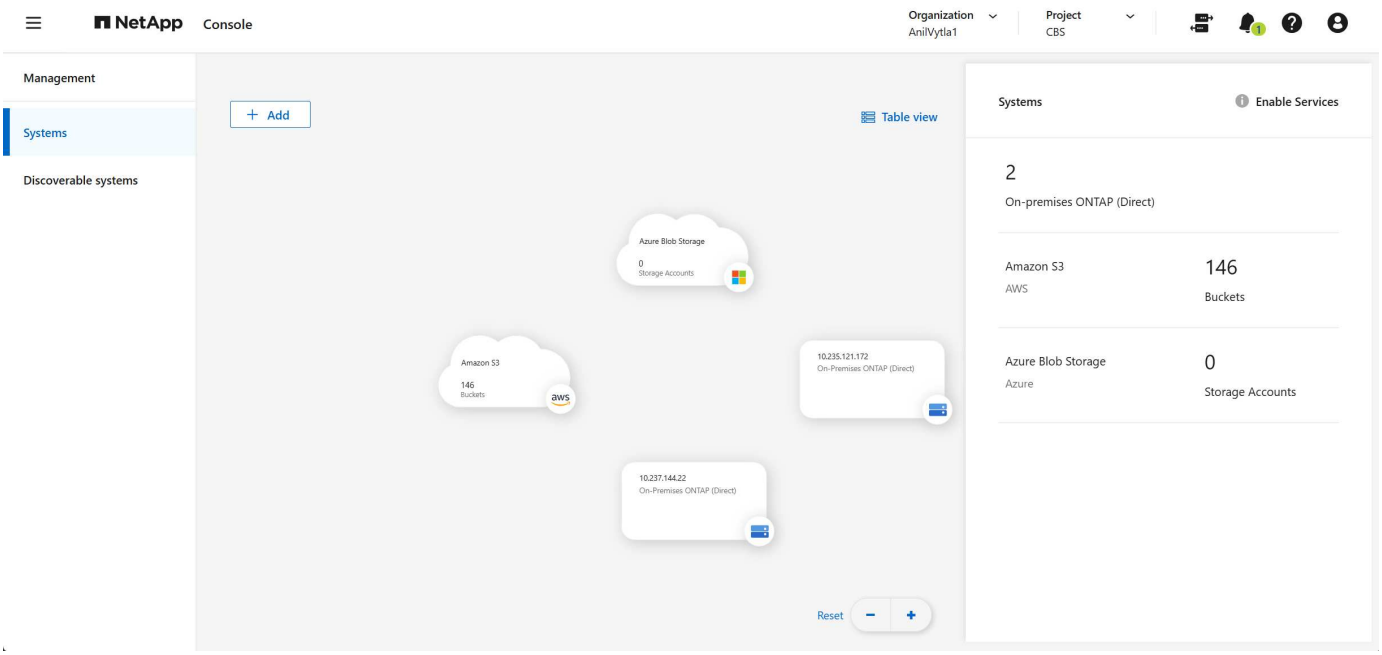
La NetApp Console, construida sobre la base BlueXP mejorada y reestructurada, proporciona una gestión centralizada del almacenamiento de NetApp y de los NetApp Data Services en entornos locales y en la nube a nivel empresarial, brindando información en tiempo real, flujos de trabajo más rápidos y una administración simplificada que es altamente segura y compatible.

Menús y páginas de navegación

NetApp movió la mayoría de las opciones del menú al panel de navegación izquierdo y reorganizó los menús para facilitar la navegación en la NetApp Console.

Canvas se reemplaza por la página de Sistemas

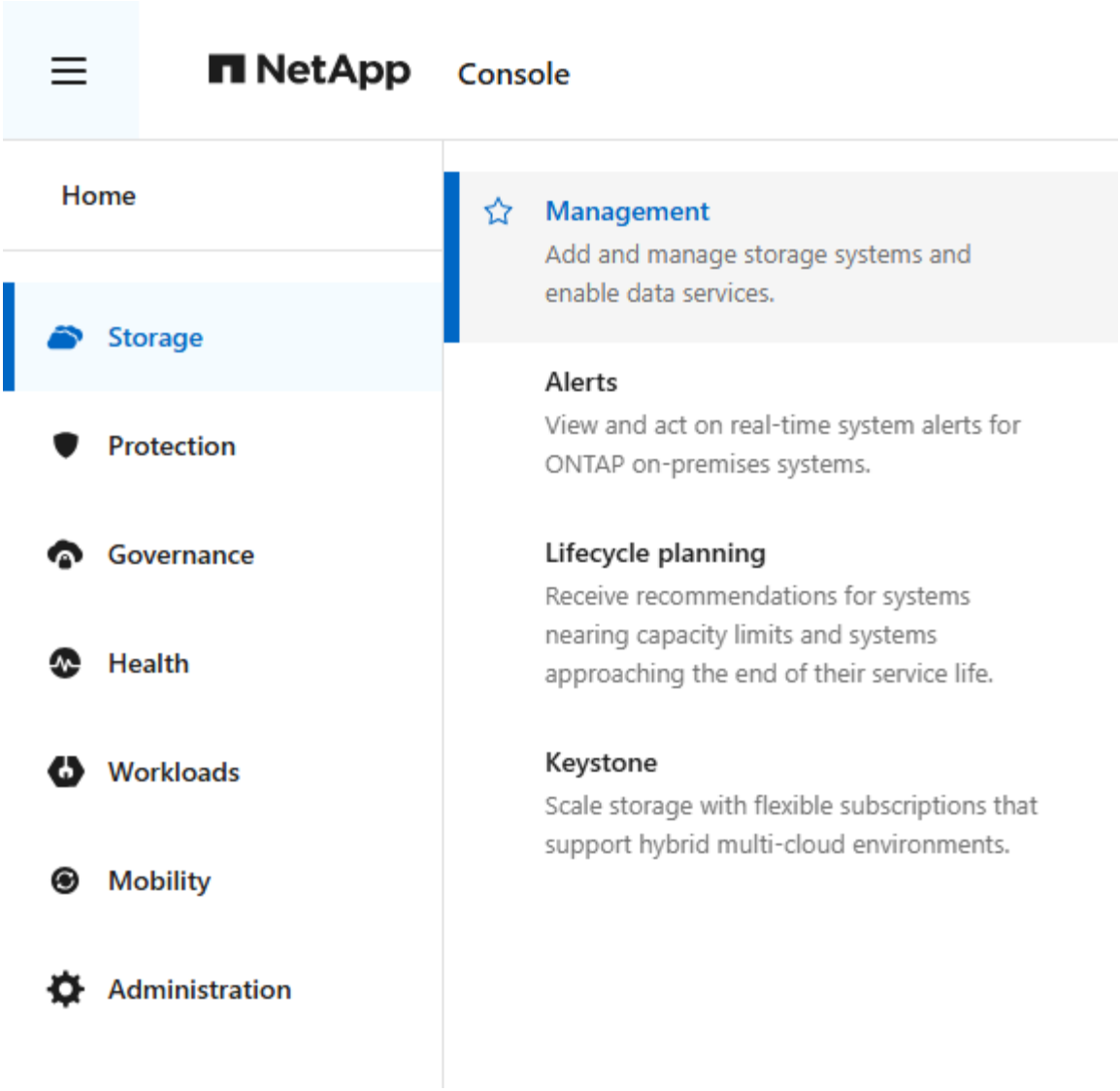
NetApp cambió el nombre del Canvas a la página **Sistemas**. Vaya a la página **Sistemas** desde el menú **Almacenamiento > Administración**.



Menú de almacenamiento ampliado

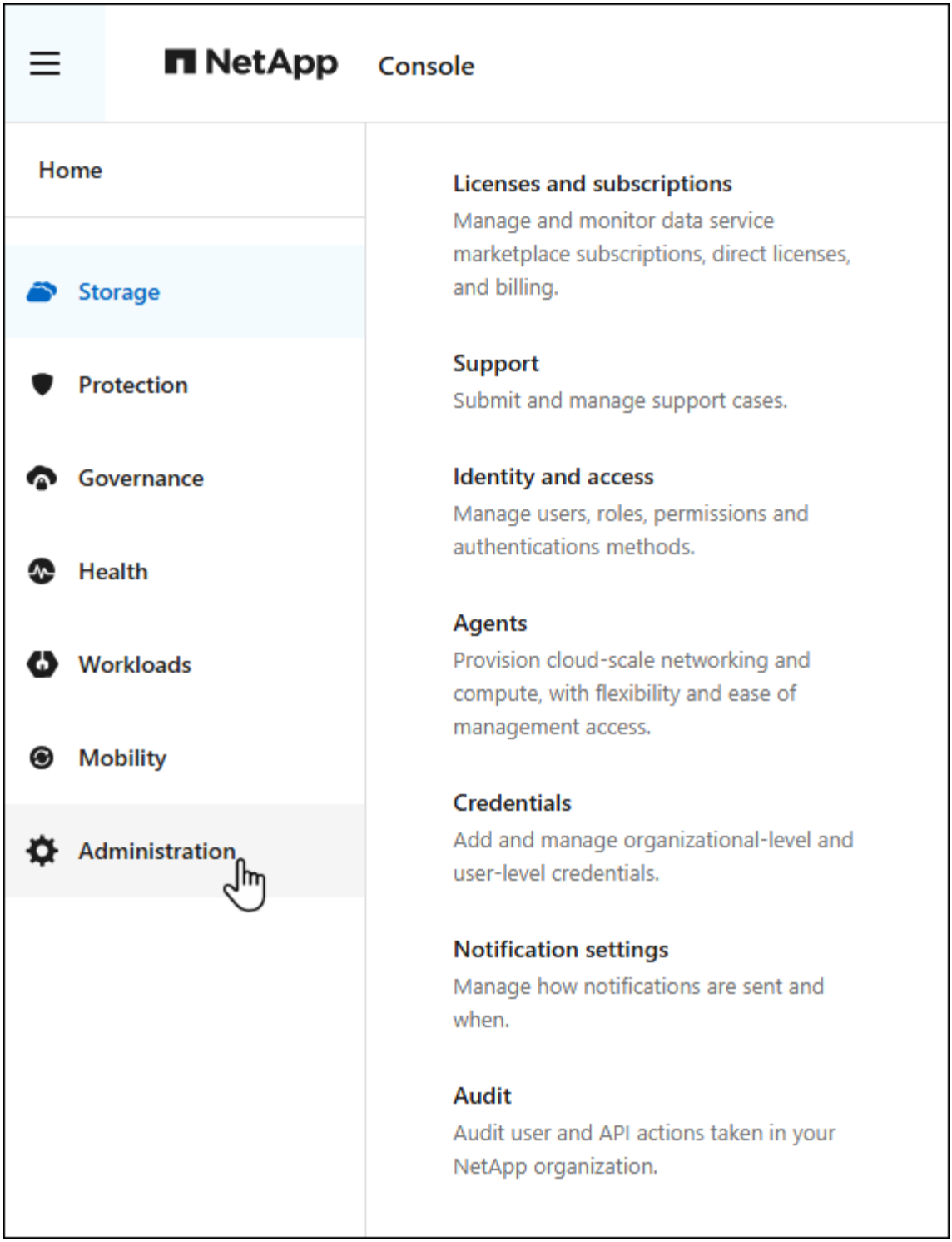
El menú **Almacenamiento** incluye **Alertas** para ver las alertas del sistema ONTAP y **Planificación del ciclo de vida** (anteriormente **Eficiencia económica**) para identificar recursos no utilizados o subutilizados.

NetApp ha movido Keystone al menú **Almacenamiento**, donde puede administrar sus suscripciones de NetApp Keystone y ver su uso.



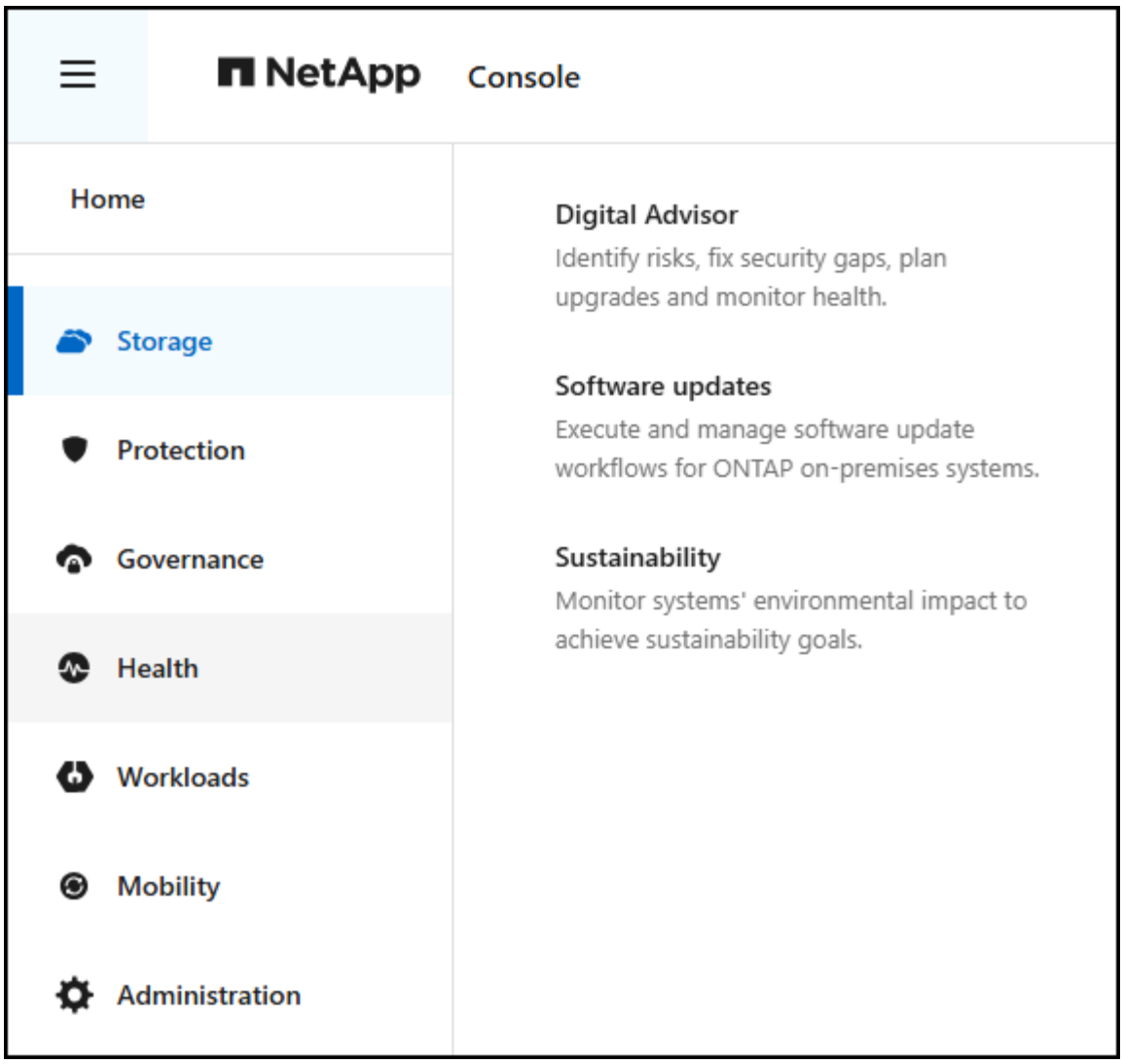
Menú de administración

Utilice el menú centralizado **Administración** para administrar la NetApp Console, los casos de soporte, las licencias y las suscripciones (anteriormente llamadas billetera digital).



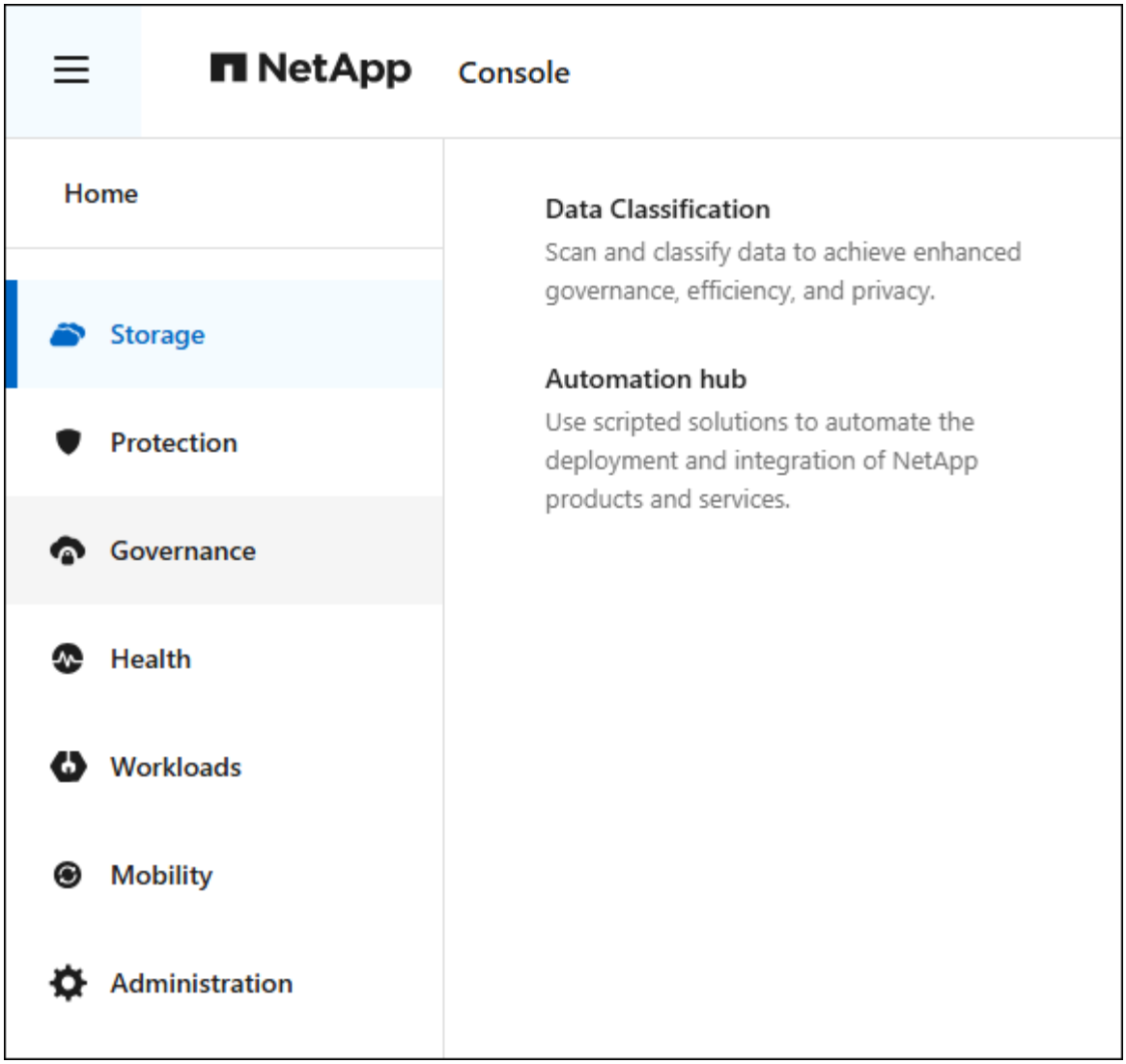
Menú de salud

Un menú **Salud** eficiente incluye **Actualizaciones de software** donde puede administrar las actualizaciones del software ONTAP , **Sustentabilidad** donde puede monitorear su impacto ambiental y * Digital Advisor* donde puede obtener recomendaciones proactivas para optimizar su entorno de almacenamiento.



Menú de gobernanza

El menú **Gobernanza** incluye **Clasificación de datos**, donde puede administrar la clasificación y el cumplimiento de los datos, y el **Centro de automatización**, donde puede crear y administrar flujos de trabajo de automatización.



Nomenclatura más intuitiva de elementos, servicios de datos y funciones

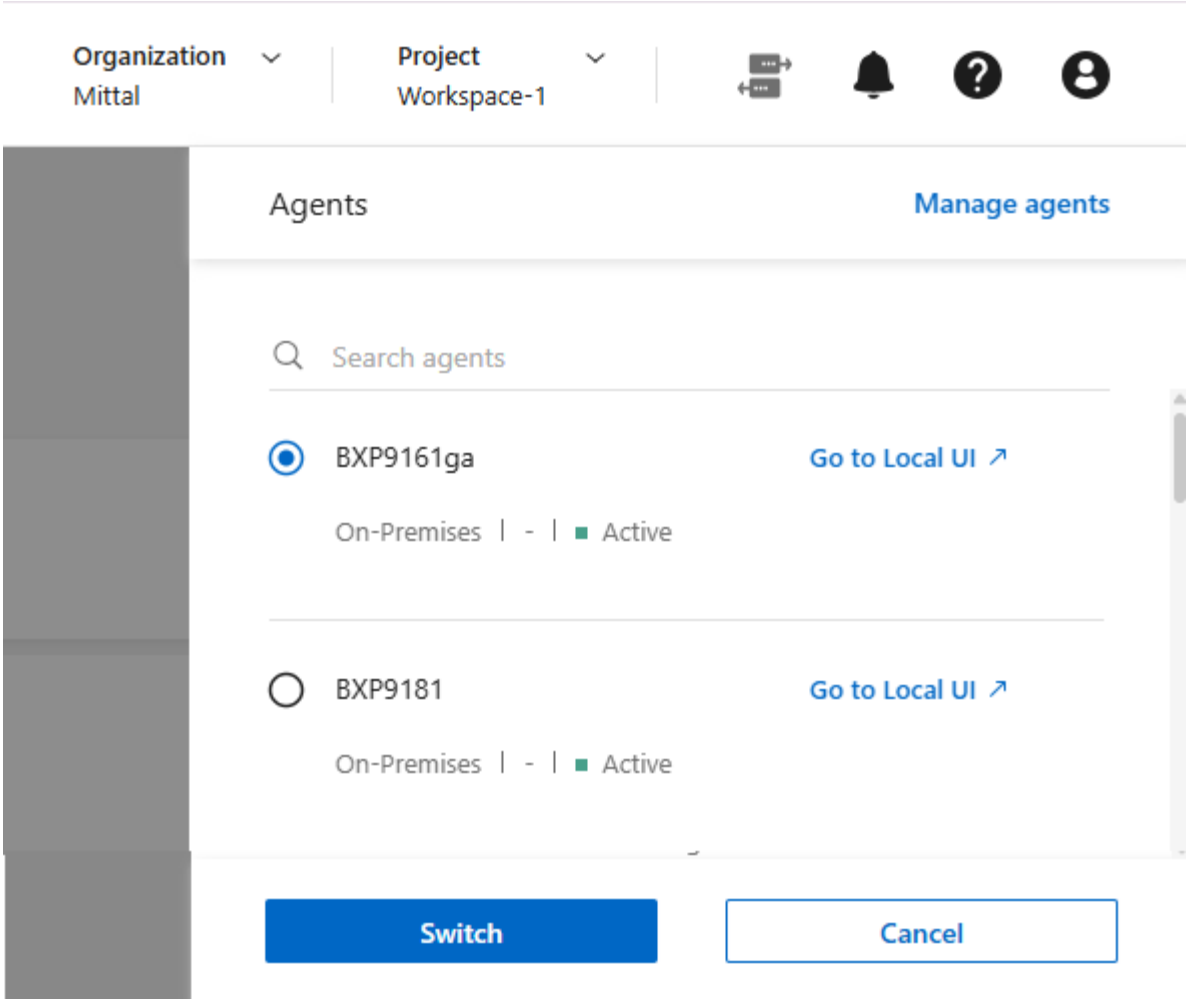
NetApp cambió el nombre de varios elementos, servicios de datos y características para aclarar su propósito. Los cambios clave incluyen:

Nombre anterior	* Nombre de la NetApp Console *
Conectores	Agentes de consola. Vea, agregue y administre sus agentes desde el menú **Administración > Agentes**.
Página de la línea de tiempo	Página de auditoría Vea la actividad de la consola de auditoría desde el menú **Administración > Auditoría**.

Nombre anterior	* Nombre de la NetApp Console *
Entornos de trabajo	Sistemas Vea, agregue y administre sus sistemas desde el menú **Almacenamiento > Administración**.
Protección contra ransomware BlueXP	NetApp Ransomware Resilience. Ransomware Resilience le ayuda a proteger sus datos y recuperarse rápidamente de un ataque de ransomware.
Eficiencia económica de BlueXP	Planificación del ciclo de vida. La planificación del ciclo de vida le ayuda a optimizar sus costos de almacenamiento al identificar recursos no utilizados y subutilizados. Acceda a la Planificación del ciclo de vida desde el menú **Almacenamiento > Planificación del ciclo de vida**.
BlueXP digital wallet	Licenses and subscriptions Acceda a sus licencias y suscripciones desde el menú **Administración > Licenses and subscriptions**.

Agentes de consola

Acceda y administre sus agentes de consola desde el menú **Administración > Agentes**. NetApp ha cambiado la forma de seleccionar un agente de consola para la página **Sistemas** (anteriormente Canvas). NetApp ha reemplazado el nombre del menú Conector por un ícono , lo que le permite seleccionar el agente de consola para el cual desea ver los sistemas.



También puedes administrar tus agentes desde el menú **Administración > Agentes**.

Agente de consola 4.0.0

Esta versión del agente de consola incluye mejoras de seguridad, correcciones de errores y las siguientes características nuevas.

La versión 4.0.0 está disponible para el modo estándar y el modo restringido.

Consolidación y reducción de los puntos finales de red necesarios

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

- "Aprenda cómo actualizar su lista de puntos de conexión y vea una comparación.".
- "Obtenga más información sobre los puntos finales necesarios."

Compatibilidad con la implementación de agentes de consola en VCenter

Puede implementar agentes de consola en entornos VMware mediante un archivo OVA. El archivo OVA incluye una imagen de VM preconfigurada con el software del agente de consola y configuraciones para conectarse a la NetApp Console. La descarga de un archivo o la implementación de una URL está disponible directamente desde la NetApp Console."Aprenda a implementar un agente de consola en entornos VMware."

El agente de consola OVA para VMware ofrece una imagen de VM preconfigurada para una implementación rápida.

Informes de validación para implementaciones de agentes fallidas

Al implementar un agente de consola desde la NetApp Console, ahora tiene la opción de validar la configuración del agente. Si la consola no logra implementar el agente, proporciona un informe descargable para ayudarlo a solucionar el problema.

Solución de problemas mejorada para los agentes de la consola

El agente de consola ha mejorado los mensajes de error que le ayudan a comprender mejor los problemas."Aprenda a solucionar problemas de los agentes de la consola."

NetApp Console

La administración de la NetApp Console incluye las siguientes características nuevas:

Panel de control de la página de inicio

El panel de la página de inicio de la consola de NetApp proporciona visibilidad en tiempo real de la infraestructura de almacenamiento con métricas de estado, capacidad, estado de la licencia y servicios de datos."Obtenga más información sobre la página de inicio."

Asistente de NetApp

Los nuevos usuarios con el rol de administrador de la organización pueden usar el asistente de NetApp para configurar la consola, lo que incluye agregar un agente, vincular una cuenta de soporte de NetApp y agregar un sistema de almacenamiento."Obtenga más información sobre el asistente de NetApp ."

Autenticación de cuenta de servicio

La NetApp Console admite la autenticación de cuentas de servicio mediante un ID de cliente generado por el sistema y un secreto o JWT administrados por el cliente, lo que permite a las organizaciones seleccionar el enfoque que mejor se adapte a sus requisitos de seguridad y flujos de trabajo de integración. La autenticación de cliente JWT de clave privada utiliza criptografía asimétrica, lo que proporciona una seguridad más fuerte que los métodos secretos e identificadores de cliente tradicionales. La autenticación de cliente JWT de clave privada utiliza criptografía asimétrica, lo que mantiene la clave privada segura en el entorno del cliente, reduce los riesgos de robo de credenciales y mejora la seguridad de su pila de automatización y aplicaciones cliente."Aprenda cómo agregar una cuenta de servicio."

Tiempos de espera de sesión

El sistema cierra la sesión de los usuarios después de 24 horas o cuando cierran su navegador web.

Apoyo a las alianzas entre organizaciones

Puede crear asociaciones en la NetApp Console que permitan a los socios administrar de forma segura los recursos de NetApp a través de los límites organizacionales, lo que facilita la colaboración y fortalece la seguridad. "Aprenda a gestionar las asociaciones" .

Roles de superadministrador y supervisor

Se agregaron los roles de **Superadministrador** y **Supervisor**. **Superadministrador** otorga acceso de gestión completo a las funciones de la consola, el almacenamiento y los servicios de datos. **Super visor** proporciona visibilidad de solo lectura para auditores y partes interesadas. Estos roles son útiles para equipos más pequeños con miembros senior donde el acceso amplio es común. Para mejorar la seguridad y la auditabilidad, se recomienda a las organizaciones utilizar el acceso de **Superadministrador** con moderación y asignar roles específicos siempre que sea posible."Obtenga más información sobre los roles de acceso."

Rol adicional para la resiliencia frente al ransomware

Se agregó el rol **Administrador de comportamiento del usuario de Ransomware Resilience** y el rol **Visor de comportamiento del usuario de Ransomware Resilience**. Estos roles permiten a los usuarios configurar y ver el comportamiento del usuario y los datos analíticos, respectivamente."Obtenga más información sobre los roles de acceso."

Se eliminó el chat de soporte

NetApp ha eliminado la función de chat de soporte de la NetApp Console. Utilice la página **Administración > Soporte** para crear y administrar casos de soporte.

11 de agosto de 2025

Conector 3.9.55

Esta versión del conector BlueXP incluye mejoras de seguridad y correcciones de errores.

La versión 3.9.55 está disponible para el modo estándar y el modo restringido.

Compatibilidad con el idioma japonés

La interfaz de usuario de BlueXP ahora está disponible en idioma japonés. Si el idioma de su navegador es japonés, BlueXP se muestra en japonés. Para acceder a la documentación en japonés, utilice el menú de idioma en el sitio web de la documentación.

Característica de resiliencia operativa

La función de resiliencia operativa se ha eliminado de BlueXP. Comuníquese con el soporte de NetApp si tiene problemas.

Gestión de identidad y acceso (IAM) de BlueXP

La gestión de identidad y acceso en BlueXP ahora ofrece la siguiente característica.

Nuevo rol de acceso para soporte operativo

BlueXP ahora admite un rol de analista de soporte operativo. Esta función otorga a un usuario permisos para supervisar alertas de almacenamiento, ver la línea de tiempo de auditoría de BlueXP e ingresar y rastrear

casos de soporte de NetApp .

"Obtenga más información sobre el uso de roles de acceso."

31 de julio de 2025

Lanzamiento del modo privado (3.9.54)

Ya está disponible para descargar un nuevo modo privado desde "Sitio de soporte de NetApp"

La versión 3.9.54 incluye actualizaciones para los siguientes componentes y servicios de BlueXP .

Componente o servicio	Versión incluida en este lanzamiento	Cambios desde el lanzamiento anterior del modo privado
Conector	3.9.54, 3.9.53	Ir a la "Novedades en la página de BlueXP" y consulte los cambios incluidos para las versiones 3.9.54 y 3.9.53.
Copia de seguridad y recuperación	28 de julio de 2025	Ir a la "Novedades en la página de BlueXP backup and recovery" y consulte los cambios incluidos en la versión de julio de 2025.
Clasificación	14 de julio de 2025 (versión 1.45)	Ir a la "Novedades en la página de BlueXP classification" .

Para obtener más detalles sobre el modo privado, incluido cómo actualizarlo, consulta lo siguiente:

- "Conozca el modo privado"
- "Aprenda cómo comenzar a usar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"

21 de julio de 2025

Compatibilidad con Google Cloud NetApp Volumes

Ahora puedes ver Google Cloud NetApp Volumes en BlueXP."Obtenga más información sobre Google Cloud NetApp Volumes."

Gestión de identidad y acceso (IAM) de BlueXP

Nuevo rol de acceso para Google Cloud NetApp Volumes

BlueXP ahora admite el uso de un rol de acceso para el siguiente sistema de almacenamiento:

- Google Cloud NetApp Volumes

"Obtenga más información sobre el uso de roles de acceso."

14 de julio de 2025

Conector 3.9.54

Esta versión del conector BlueXP incluye mejoras de seguridad, correcciones de errores y las siguientes características nuevas:

- Compatibilidad con servidores proxy transparentes para conectores dedicados a respaldar los servicios de Cloud Volumes ONTAP ."Obtenga más información sobre cómo configurar un proxy transparente."
- Capacidad de usar etiquetas de red para ayudar a enrutar el tráfico del conector cuando este se implementa en un entorno de Google Cloud.
- Notificaciones adicionales dentro del producto para la monitorización del estado del conector, incluido el uso de CPU y RAM.

En este momento, la versión 3.9.54 está disponible para el modo estándar y el modo restringido.

Gestión de identidad y acceso (IAM) de BlueXP

La gestión de identidad y acceso en BlueXP ahora ofrece las siguientes funciones:

- Soporte para IAM en modo privado, lo que le permite administrar el acceso de los usuarios y los permisos para los servicios y aplicaciones de BlueXP .
- Gestión optimizada de federaciones de identidad, que incluye una navegación más sencilla, opciones más claras para configurar conexiones federadas y una mejor visibilidad de las federaciones existentes.
- Roles de acceso para BlueXP backup and recovery, BlueXP disaster recovery y administración de federación.

Compatibilidad con IAM en modo privado

BlueXP ahora admite IAM en modo privado, lo que le permite administrar el acceso de los usuarios y los permisos para los servicios y aplicaciones de BlueXP . Esta mejora permite a los clientes del modo privado aprovechar el control de acceso basado en roles (RBAC) para lograr una mejor seguridad y cumplimiento.

"Obtenga más información sobre IAM en BlueXP."

Gestión optimizada de federaciones de identidad

BlueXP ahora ofrece una interfaz más intuitiva para administrar la federación de identidad. Esto incluye una navegación más sencilla, opciones más claras para configurar conexiones federadas y una mejor visibilidad de las federaciones existentes.

Habilitar el inicio de sesión único (SSO) a través de la federación de identidad permite a los usuarios iniciar sesión en BlueXP con sus credenciales corporativas. Esto mejora la seguridad, reduce el uso de contraseñas y simplifica la incorporación.

Se le pedirá que importe cualquier conexión federada existente a la nueva interfaz para obtener acceso a las nuevas funciones de administración. Esto le permite aprovechar las últimas mejoras sin tener que recrear sus conexiones federadas."Obtenga más información sobre cómo importar su conexión federada existente a BlueXP."

Una gestión mejorada de la federación le permite:

- Agregue más de un dominio verificado a una conexión federada, lo que le permitirá utilizar múltiples

dominios con el mismo proveedor de identidad (IdP).

- Deshabilite o elimine las conexiones federadas cuando sea necesario, lo que le otorgará control sobre el acceso y la seguridad de los usuarios.
- Controle el acceso a la gestión de la federación con roles de IAM.

"Obtenga más información sobre la federación de identidad en BlueXP."

Nuevos roles de acceso para la BlueXP backup and recovery, la BlueXP disaster recovery y la administración de la federación

BlueXP ahora admite el uso de roles IAM para las siguientes funciones y servicios de datos:

- BlueXP backup and recovery
- BlueXP disaster recovery
- Federación

"Obtenga más información sobre el uso de roles de acceso."

9 de junio de 2025

Conector 3.9.53

Esta versión del conector BlueXP incluye mejoras de seguridad y correcciones de errores.

La versión 3.9.53 está disponible para el modo estándar y el modo restringido.

Alertas de uso de espacio en disco

El Centro de notificaciones ahora incluye alertas sobre el uso del espacio en disco en el Conector."Más información."

Mejoras en la auditoría

La línea de tiempo ahora incluye eventos de inicio y cierre de sesión para los usuarios. Puede ver cuándo hay actividad de inicio de sesión, lo que puede ayudar con la auditoría y el monitoreo de seguridad. Los usuarios de API que tienen el rol de administrador de la organización pueden ver la dirección de correo electrónico del usuario que inició sesión al incluir el `includeUserData=true` parámetro como en el siguiente: `/audit/<account_id>?includeUserData=true` .

Gestión de suscripciones de Keystone disponible en BlueXP

Puede administrar su suscripción a NetApp Keystone desde BlueXP.

"Obtenga información sobre la gestión de suscripciones de Keystone en BlueXP."

Gestión de identidad y acceso (IAM) de BlueXP

Autenticación multifactor (MFA)

Los usuarios no federados pueden habilitar MFA para sus cuentas BlueXP para mejorar la seguridad. Los administradores pueden gestionar la configuración de MFA, incluido el restablecimiento o la desactivación de MFA para los usuarios según sea necesario. Esto solo es compatible en el modo estándar.

"Obtenga información sobre cómo configurar la autenticación multifactor para usted." "Obtenga información sobre cómo administrar la autenticación multifactor para los usuarios."

Cargas de trabajo

Ahora puede ver y eliminar las credenciales de Amazon FSx for NetApp ONTAP desde la página Credenciales en BlueXP.

29 de mayo de 2025

Lanzamiento del modo privado (3.9.52)

Ya está disponible para descargar un nuevo modo privado desde "Sitio de soporte de NetApp"

La versión 3.9.52 incluye actualizaciones para los siguientes componentes y servicios de BlueXP .

Componente o servicio	Versión incluida en este lanzamiento	Cambios desde el lanzamiento anterior del modo privado
Conector	3.9.52, 3.9.51	Ir a la "Novedades en la página del conector BlueXP" y consulte los cambios incluidos para las versiones 3.9.52 y 3.9.50.
Copia de seguridad y recuperación	12 de mayo de 2025	Ir a la "Novedades en la página de BlueXP backup and recovery" y consulte los cambios incluidos en la versión de mayo de 2025.
Clasificación	12 de mayo de 2025 (versión 1.43)	Ir a la "Novedades en la página de BlueXP classification" y consulte los cambios incluidos en las versiones 1.38 a 1.371.41.

Para obtener más detalles sobre el modo privado, incluido cómo actualizarlo, consulta lo siguiente:

- "Conozca el modo privado"
- "Aprenda cómo comenzar a usar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"

12 de mayo de 2025

Conector 3.9.52

Esta versión del conector BlueXP incluye pequeñas mejoras de seguridad y correcciones de errores, así como algunas actualizaciones adicionales.

En este momento, la versión 3.9.52 está disponible para el modo estándar y el modo restringido.

Compatibilidad con Docker 27 y Docker 28

Docker 27 y Docker 28 ahora son compatibles con el Conector.

Cloud Volumes ONTAP

Los nodos de Cloud Volumes ONTAP ya no se apagan cuando el conector no cumple con las normas o permanece inactivo durante más de 14 días. Cloud Volumes ONTAP aún envía mensajes de administración de eventos cuando pierde acceso al conector. Este cambio tiene como objetivo garantizar que Cloud Volumes ONTAP pueda seguir funcionando incluso si el conector está inactivo durante un período prolongado. No cambia los requisitos de cumplimiento del Conector.

Administración de Keystone disponible en BlueXP

La versión beta de NetApp Keystone en BlueXP agregó acceso a la administración de Keystone . Puede acceder a la página de registro para la versión beta de NetApp Keystone desde la barra de navegación izquierda de BlueXP.

Gestión de identidad y acceso (IAM) de BlueXP

Nuevas funciones de gestión de almacenamiento

Los roles de administrador de almacenamiento, especialista en estado del sistema y visualizador de almacenamiento están disponibles y se pueden asignar a los usuarios.

Estos roles le permiten administrar quién en su organización puede descubrir y administrar recursos de almacenamiento, así como ver información sobre el estado del almacenamiento y realizar actualizaciones de software.

Estos roles son compatibles para controlar el acceso a los siguientes recursos de almacenamiento:

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

También puede utilizar estos roles para controlar el acceso a los siguientes servicios de BlueXP :

- Actualizaciones de software
- Asesor digital
- Resiliencia operativa
- Eficiencia económica
- Sostenibilidad

Se han añadido los siguientes roles:

- **Administrador de almacenamiento**

  Administrar la salud del almacenamiento, la gobernanza y el descubrimiento de los recursos de almacenamiento en la organización. Esta función también puede realizar actualizaciones de software en recursos de almacenamiento.

- **Especialista en salud del sistema**

  Administrar la salud y la gobernanza del almacenamiento de los recursos de almacenamiento en la organización. Esta función también puede realizar actualizaciones de software en recursos de almacenamiento. Este rol no puede modificar ni eliminar entornos de trabajo.

- **Visor de almacenamiento**

  Ver información sobre el estado del almacenamiento y datos de gobernanza.

  "Obtenga más información sobre los roles de acceso."

14 de abril de 2025

Conector 3.9.51

Esta versión del conector BlueXP incluye pequeñas mejoras de seguridad y correcciones de errores.

En este momento, la versión 3.9.51 está disponible para el modo estándar y el modo restringido.

Los puntos finales seguros para descargas de conectores ahora son compatibles con copias de seguridad, recuperación y protección contra ransomware.

Si utiliza copia de seguridad y recuperación o protección contra ransomware, ahora puede usar puntos finales seguros para las descargas de conectores."Obtenga información sobre los puntos finales seguros para las descargas de Connector."

Gestión de identidad y acceso (IAM) de BlueXP

- A los usuarios que no sean administradores de organización, carpeta o proyecto se les debe asignar un rol de protección contra ransomware para tener acceso a dicha protección. Puede asignar a un usuario uno de dos roles: administrador de protección contra ransomware o visor de protección contra ransomware.
- A los usuarios que no sean administradores de organización, carpeta o proyecto se les debe asignar un rol de Keystone para tener acceso a Keystone. Puede asignar a un usuario uno de dos roles: administrador de Keystone o visor de Keystone .

  "Obtenga más información sobre los roles de acceso."

- Si tiene el rol de administrador de organización, de carpeta o de proyecto, ahora puede asociar una suscripción de Keystone con un proyecto de IAM. Asociar una suscripción de Keystone con un proyecto IAM le permite controlar el acceso a Keystone dentro de BlueXP.

28 de marzo de 2025

Lanzamiento del modo privado (3.9.50)

Ya está disponible para descargar un nuevo modo privado desde "Sitio de soporte de NetApp"

La versión 3.9.50 incluye actualizaciones para los siguientes componentes y servicios de BlueXP .

Componente o servicio	Versión incluida en este lanzamiento	Cambios desde el lanzamiento anterior del modo privado
Conector	3.9.50, 3.9.49	Ir a la "Novedades en la página del conector BlueXP" y consulte los cambios incluidos para las versiones 3.9.50 y 3.9.49.

Componente o servicio	Versión incluida en este lanzamiento	Cambios desde el lanzamiento anterior del modo privado
Copia de seguridad y recuperación	17 de marzo de 2025	Ir a la "Novedades en la página de BlueXP backup and recovery" y consulte los cambios incluidos en la versión de marzo de 2024.
Clasificación	10 de marzo de 2025 (versión 1.41)	Ir a la "Novedades en la página de BlueXP classification" y consulte los cambios incluidos en las versiones 1.38 a 1.371.41.

Para obtener más detalles sobre el modo privado, incluido cómo actualizarlo, consulta lo siguiente:

- "Conozca el modo privado"
- "Aprenda cómo comenzar a usar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"

10 de marzo de 2025

Conector 3.9.50

Esta versión del conector BlueXP incluye pequeñas mejoras de seguridad y correcciones de errores.

- La administración de los sistemas Cloud Volumes ONTAP ahora es compatible con conectores que tienen SELinux habilitado en el sistema operativo.

  "Obtenga más información sobre SELinux"

En este momento, la versión 3.9.50 está disponible para el modo estándar y el modo restringido.

La versión beta de NetApp Keystone está disponible en BlueXP

NetApp Keystone pronto estará disponible en BlueXP y ahora está en versión beta. Puede acceder a la página de registro para la versión beta de NetApp Keystone desde la barra de navegación izquierda de BlueXP.

6 de marzo de 2025

Actualización del conector 3.9.49

Acceso al Administrador del sistema ONTAP cuando BlueXP utiliza un conector

Un administrador de BlueXP (usuarios con el rol de administrador de la organización) puede configurar BlueXP para solicitar a los usuarios que ingresen sus credenciales de ONTAP para acceder al administrador del sistema de ONTAP . Cuando esta configuración está habilitada, los usuarios deben ingresar sus credenciales de ONTAP cada vez, ya que no se almacenan en BlueXP.

Esta función está disponible en la versión 3.9.49 y superiores del Conector. "Aprenda a configurar los ajustes de credenciales." .

18 de febrero de 2025

Lanzamiento del modo privado (3.9.48)

Ya está disponible para descargar un nuevo modo privado desde "Sitio de soporte de NetApp"

La versión 3.9.48 incluye actualizaciones para los siguientes componentes y servicios de BlueXP .

Componente o servicio	Versión incluida en este lanzamiento	Cambios desde el lanzamiento anterior del modo privado
Conector	3.9.48	Ir a la "Novedades en la página del conector BlueXP" y consulte los cambios incluidos para las versiones 3.9.48.
Copia de seguridad y recuperación	21 de febrero de 2025	Ir a la "Novedades en la página de BlueXP backup and recovery" y consulte los cambios incluidos en la versión de febrero de 2025.
Clasificación	22 de enero de 2025 (versión 1.39)	Ir a la "Novedades en la página de BlueXP classification" y consulte los cambios incluidos en la versión 1.39.

10 de febrero de 2025

Conector 3.9.49

Esta versión del conector BlueXP incluye pequeñas mejoras de seguridad y correcciones de errores.

En este momento, la versión 3.9.49 está disponible para el modo estándar y el modo restringido.

Gestión de identidad y acceso (IAM) de BlueXP

- Soporte para asignar múltiples roles a un usuario de BlueXP .
- Soporte para asignar un rol en múltiples recursos de la organización BlueXP (Organización/Carpeta/Proyecto)
- Los roles ahora están asociados con una de dos categorías: plataforma y servicio de datos.

El modo restringido ahora usa BlueXP IAM

La gestión de identidad y acceso (IAM) de BlueXP ahora se utiliza en modo restringido.

La gestión de identidad y acceso (IAM) de BlueXP es un modelo de gestión de recursos y acceso que reemplaza y mejora la funcionalidad anterior proporcionada por las cuentas de BlueXP cuando se utiliza BlueXP en modo estándar y restringido.

Información relacionada

- "Obtenga más información sobre BlueXP IAM"
- "Comience a utilizar BlueXP IAM"

BlueXP IAM proporciona una gestión más granular de recursos y permisos:

- Una *organización* de nivel superior le permite administrar el acceso a sus diversos *proyectos*.
- Las *carpetas* le permiten agrupar proyectos relacionados.
- La gestión mejorada de recursos le permite asociar un recurso con una o más carpetas o proyectos.

  Por ejemplo, puede asociar un sistema Cloud Volumes ONTAP con múltiples proyectos.

- La gestión de acceso mejorada le permite asignar un rol a los miembros en diferentes niveles de la jerarquía de la organización.

Estas mejoras proporcionan un mejor control sobre las acciones que los usuarios pueden realizar y los recursos a los que pueden acceder.

Cómo afecta BlueXP IAM a su cuenta existente en modo restringido

Cuando inicie sesión en BlueXP, notará estos cambios:

- Su *cuenta* ahora se llama *organización*
- Tus *espacios de trabajo* ahora se llaman *proyectos*
- Los nombres de los roles de usuario han cambiado:
  - *Administrador de cuenta* ahora es *Administrador de organización*
  - *Administrador del espacio de trabajo* ahora es *Administrador de carpeta o proyecto*
  - *Visor de cumplimiento* ahora es *Visor de clasificación*
- En Configuración, puede acceder a la gestión de identidad y acceso de BlueXP para aprovechar estas mejoras.

Tenga en cuenta lo siguiente:

- No hay cambios en sus usuarios o entornos de trabajo existentes.
- Si bien los nombres de los roles han cambiado, no hay diferencias desde la perspectiva de permisos. Los usuarios seguirán teniendo acceso a los mismos entornos de trabajo que antes.
- No hay cambios en la forma de iniciar sesión en BlueXP. BlueXP IAM funciona con inicios de sesión en la nube de NetApp , credenciales del sitio de soporte de NetApp y conexiones federadas tal como lo hacían las cuentas de BlueXP .
- Si tenía varias cuentas BlueXP , ahora tiene varias organizaciones BlueXP .

API para BlueXP IAM

Este cambio introduce una nueva API para BlueXP IAM, pero es compatible con versiones anteriores de la API de arrendamiento. "Obtenga más información sobre la API para BlueXP IAM"

Modos de implementación admitidos

BlueXP IAM es compatible cuando se utiliza BlueXP en modo estándar y restringido. Si usa BlueXP en modo privado, continuará usando una *cuenta* de BlueXP para administrar espacios de trabajo, usuarios y recursos.

Lanzamiento del modo privado (3.9.48)

Ya está disponible para descargar un nuevo modo privado desde "Sitio de soporte de NetApp"

La versión 3.9.48 incluye actualizaciones para los siguientes componentes y servicios de BlueXP .

Componente o servicio	Versión incluida en este lanzamiento	Cambios desde el lanzamiento anterior del modo privado
Conector	3.9.48	Ir a la "Novedades en la página del conector BlueXP" y consulte los cambios incluidos para las versiones 3.9.48.
Copia de seguridad y recuperación	21 de febrero de 2025	Ir a la "Novedades en la página de BlueXP backup and recovery" y consulte los cambios incluidos en la versión de febrero de 2025.
Clasificación	22 de enero de 2025 (versión 1.39)	Ir a la "Novedades en la página de BlueXP classification" y consulte los cambios incluidos en la versión 1.39.

13 de enero de 2025

Conector 3.9.48

Esta versión del conector BlueXP incluye pequeñas mejoras de seguridad y correcciones de errores.

En este momento, la versión 3.9.48 está disponible para el modo estándar y el modo restringido.

Gestión de identidad y acceso de BlueXP

- La página Recursos ahora muestra recursos no descubiertos. Los recursos no descubiertos son recursos de almacenamiento que BlueXP conoce pero para los cuales no ha creado entornos de trabajo. Por ejemplo, los recursos que se muestran en el asesor digital y que aún no tienen entornos de trabajo se muestran en la página Recursos como recursos no descubiertos.
- Los recursos de Amazon FSx for NetApp ONTAP no se muestran en la página de recursos de IAM porque no es posible asociarlos con una función de IAM. Puede ver estos recursos en su lienzo respectivo o desde las cargas de trabajo.

Cree un caso de soporte para servicios adicionales de BlueXP

Después de registrar BlueXP para recibir soporte, puede crear un caso de soporte directamente desde la consola web de BlueXP . Al crear el caso, debe seleccionar el servicio con el que está asociado el problema.

A partir de esta versión, ahora puede crear un caso de soporte y asociarlo con servicios BlueXP adicionales:

- BlueXP disaster recovery
- BlueXP ransomware protection

"Obtenga más información sobre cómo crear un caso de soporte" .

16 de diciembre de 2024

Nuevos puntos finales seguros para obtener imágenes del conector

Cuando instala el Conector, o cuando se produce una actualización automática, el Conector se comunica con los repositorios para descargar imágenes para la instalación o actualización. De forma predeterminada, el

conector siempre se ha puesto en contacto con los siguientes puntos finales:

- https://*.blob.core.windows.net
- \ https://cloudmanagerinfraprod.azurecr.io

El primer punto final incluye un comodín porque no podemos proporcionar una ubicación definitiva. El equilibrio de carga del repositorio lo gestiona el proveedor de servicios, lo que significa que las descargas pueden realizarse desde diferentes puntos finales.

Para mayor seguridad, el Conector ahora puede descargar imágenes de instalación y actualizaciones desde puntos finales dedicados:

- \ https://bluexpinfraprod.eastus2.data.azurecr.io
- \ https://bluexpinfraprod.azurecr.io

Le recomendamos que comience a utilizar estos nuevos puntos finales eliminando los puntos finales existentes de sus reglas de firewall y permitiendo los nuevos puntos finales.

Estos nuevos puntos finales son compatibles a partir de la versión 3.9.47 del Conector. No hay compatibilidad con versiones anteriores del Conector.

Tenga en cuenta lo siguiente:

- Los puntos finales existentes aún reciben soporte. Si no desea utilizar los nuevos puntos finales, no es necesario realizar ningún cambio.
- El conector contacta primero los puntos finales existentes. Si esos puntos finales no son accesibles, el Conector contacta automáticamente los nuevos puntos finales.
- Los nuevos puntos finales no son compatibles con los siguientes escenarios:
  - Si el conector está instalado en una región gubernamental.
  - Si utiliza el Conector con la BlueXP backup and recovery o la BlueXP ransomware protection.

  Para ambos escenarios, puede seguir utilizando los puntos finales existentes.

9 de diciembre de 2024

Conector 3.9.47

Esta versión del conector BlueXP incluye correcciones de errores y un cambio en los puntos finales contactados durante la instalación del conector.

En este momento, la versión 3.9.47 está disponible para el modo estándar y el modo restringido.

Punto final para contactar con el soporte de NetApp durante la instalación

Cuando instala manualmente el Conector, el instalador ya no se comunica con https://support.netapp.com.

El instalador aún se comunica con https://mysupport.netapp.com.

Gestión de identidad y acceso de BlueXP

La página Conectores enumera únicamente los conectores disponibles actualmente. Ya no se muestran los conectores que has eliminado.

26 de noviembre de 2024

Lanzamiento del modo privado (3.9.46)

Ya está disponible para descargar un nuevo modo privado desde "Sitio de soporte de NetApp"

La versión 3.9.46 incluye actualizaciones para los siguientes componentes y servicios de BlueXP .

Componente o servicio	Versión incluida en este lanzamiento	Cambios desde el lanzamiento anterior del modo privado
Conector	3.9.46	Pequeñas mejoras de seguridad y corrección de errores
Copia de seguridad y recuperación	22 de noviembre de 2024	Ir a la "Novedades en la página de BlueXP backup and recovery" y consulte los cambios incluidos en la versión de noviembre de 2024
Clasificación	4 de noviembre de 2024 (versión 1.37)	Ir a la "Novedades en la página de BlueXP classification" y consulte los cambios incluidos en las versiones 1.32 a 1.37
Administración de Cloud Volumes ONTAP	11 de noviembre de 2024	Ir a la "Novedades en la página de administración de Cloud Volumes ONTAP" y consulte los cambios incluidos en las versiones de octubre de 2024 y noviembre de 2024
Gestión de clústeres ONTAP locales	26 de noviembre de 2024	Ir a la "Novedades en la página de administración de clústeres de ONTAP locales" y consulte los cambios incluidos en la versión de noviembre de 2024

Si bien la BlueXP digital wallet y la BlueXP replication también están incluidas con el modo privado, no hay cambios con respecto a la versión anterior del modo privado.

Para obtener más detalles sobre el modo privado, incluido cómo actualizarlo, consulta lo siguiente:

- "Conozca el modo privado"
- "Aprenda cómo comenzar a usar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"

11 de noviembre de 2024

Conector 3.9.46

Esta versión del conector BlueXP incluye pequeñas mejoras de seguridad y correcciones de errores.

En este momento, la versión 3.9.46 está disponible para el modo estándar y el modo restringido.

ID para proyectos IAM

Ahora puede ver el ID de un proyecto desde la gestión de identidad y acceso de BlueXP . Es posible que necesites usar el ID al realizar una llamada API.

"Aprenda cómo obtener el ID para un proyecto" .

10 de octubre de 2024

Parche del conector 3.9.45

Este parche incluye correcciones de errores.

7 de octubre de 2024

Gestión de identidad y acceso de BlueXP

La gestión de identidad y acceso (IAM) de BlueXP es un nuevo modelo de gestión de recursos y acceso que reemplaza y mejora la funcionalidad anterior proporcionada por las cuentas de BlueXP cuando se utiliza BlueXP en modo estándar.

BlueXP IAM proporciona una gestión más granular de recursos y permisos:

- Una *organización* de nivel superior le permite administrar el acceso a sus diversos *proyectos*.
- Las *carpetas* le permiten agrupar proyectos relacionados.
- La gestión mejorada de recursos le permite asociar un recurso con una o más carpetas o proyectos.

  Por ejemplo, puede asociar un sistema Cloud Volumes ONTAP con múltiples proyectos.

- La gestión de acceso mejorada le permite asignar un rol a los miembros en diferentes niveles de la jerarquía de la organización.

Estas mejoras proporcionan un mejor control sobre las acciones que los usuarios pueden realizar y los recursos a los que pueden acceder.

Cómo afecta BlueXP IAM a su cuenta existente

Cuando inicie sesión en BlueXP, notará estos cambios:

- Su *cuenta* ahora se llama *organización*
- Tus *espacios de trabajo* ahora se llaman *proyectos*
- Los nombres de los roles de usuario han cambiado:
  - *Administrador de cuenta* ahora es *Administrador de organización*
  - *Administrador del espacio de trabajo* ahora es *Administrador de carpeta o proyecto*
  - *Visor de cumplimiento* ahora es *Visor de clasificación*
- En Configuración, puede acceder a la gestión de identidad y acceso de BlueXP para aprovechar estas mejoras.

Tenga en cuenta lo siguiente:

- No hay cambios en sus usuarios o entornos de trabajo existentes.

- Si bien los nombres de los roles han cambiado, no hay diferencias desde la perspectiva de permisos. Los usuarios seguirán teniendo acceso a los mismos entornos de trabajo que antes.
- No hay cambios en la forma de iniciar sesión en BlueXP. BlueXP IAM funciona con inicios de sesión en la nube de NetApp , credenciales del sitio de soporte de NetApp y conexiones federadas tal como lo hacían las cuentas de BlueXP .
- Si tenía varias cuentas BlueXP , ahora tiene varias organizaciones BlueXP .

API para BlueXP IAM

Este cambio introduce una nueva API para BlueXP IAM, pero es compatible con versiones anteriores de la API de arrendamiento. "Obtenga más información sobre la API para BlueXP IAM"

Modos de implementación admitidos

BlueXP IAM es compatible cuando se utiliza BlueXP en modo estándar. Si utiliza BlueXP en modo restringido o modo privado, continuará usando una *cuenta* de BlueXP para administrar espacios de trabajo, usuarios y recursos.

¿A dónde ir después?

- "Obtenga más información sobre BlueXP IAM"
- "Comience a utilizar BlueXP IAM"

Conector 3.9.45

Esta versión incluye soporte ampliado del sistema operativo y corrección de errores.

La versión 3.9.45 está disponible para el modo estándar y el modo restringido.

Soporte para Ubuntu 24.04 LTS

A partir de la versión 3.9.45, BlueXP ahora admite nuevas instalaciones del Conector en hosts Ubuntu 24.04 LTS cuando se usa BlueXP en modo estándar o modo restringido.

"Ver requisitos de host del conector" .

Compatibilidad con SELinux con hosts RHEL

BlueXP ahora admite el conector con hosts Red Hat Enterprise Linux que tienen SELinux habilitado en modo de aplicación o modo permisivo.

El soporte para SELinux comienza con la versión 3.9.40 para el modo estándar y el modo restringido y con la versión 3.9.42 para el modo privado.

Tenga en cuenta las siguientes limitaciones:

- BlueXP no es compatible con SELinux con hosts Ubuntu.
- La administración de los sistemas Cloud Volumes ONTAP no es compatible con conectores que tengan SELinux habilitado en el sistema operativo.

"Obtenga más información sobre SELinux"

30 de septiembre de 2024

Lanzamiento del modo privado (3.9.44)

Ya está disponible para descargar una nueva versión del modo privado desde el sitio de soporte de NetApp .

Esta versión incluye las siguientes versiones de los componentes y servicios de BlueXP que son compatibles con el modo privado.

Servicio	Versión incluida
Conector	3.9.44
Copia de seguridad y recuperación	27 de septiembre de 2024
Clasificación	15 de mayo de 2024 (versión 1.31)
Administración de Cloud Volumes ONTAP	9 de septiembre de 2024
Monedero digital	30 de julio de 2023
Gestión de clústeres ONTAP locales	22 de abril de 2024
Replicación	18 de septiembre de 2022

Para el Conector, la versión de modo privado 3.9.44 incluye las actualizaciones introducidas en las versiones de agosto de 2024 y septiembre de 2024. Lo más destacable es el soporte para Red Hat Enterprise Linux 9.4.

Para obtener más información sobre lo que se incluye en las versiones de estos componentes y servicios de BlueXP , consulte las notas de la versión de cada servicio de BlueXP :

- "Novedades en la versión de septiembre de 2024 del Conector"
- "Novedades en la versión de agosto de 2024 del Conector"
- "Novedades en la BlueXP backup and recovery"
- "Novedades de la BlueXP classification"
- "Novedades en la gestión de Cloud Volumes ONTAP en BlueXP"

Para obtener más detalles sobre el modo privado, incluido cómo actualizarlo, consulta lo siguiente:

- "Conozca el modo privado"
- "Aprenda cómo comenzar a usar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"

9 de septiembre de 2024

Conector 3.9.44

Esta versión incluye soporte para Docker Engine 26, una mejora en los certificados SSL y correcciones de errores.

La versión 3.9.44 está disponible para el modo estándar y el modo restringido.

Compatibilidad con Docker Engine 26 con nuevas instalaciones

A partir de la versión 3.9.44 del Conector, Docker Engine 26 ahora es compatible con *nuevas* instalaciones del Conector en hosts Ubuntu.

Si tiene un conector existente creado antes del lanzamiento de la versión 3.9.44, entonces Docker Engine 25.0.5 sigue siendo la versión máxima compatible con los hosts de Ubuntu.

"Obtenga más información sobre los requisitos de Docker Engine" .

Certificado SSL actualizado para el acceso a la interfaz de usuario local

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

En esta versión, realizamos cambios en el certificado SSL para conectores nuevos y existentes:

- El nombre común del certificado ahora coincide con el nombre de host corto
- El nombre alternativo del sujeto del certificado es el nombre de dominio completo (FQDN) del equipo host

Compatibilidad con RHEL 9.4

BlueXP ahora admite la instalación del Conector en un host Red Hat Enterprise Linux 9.4 cuando se utiliza BlueXP en modo estándar o modo restringido.

El soporte para RHEL 9.4 comienza con la versión 3.9.40 del Conector.

La lista actualizada de versiones de RHEL compatibles con el modo estándar y el modo restringido ahora incluye lo siguiente:

- 8.6 a 8.10
- 9.1 a 9.4

"Obtenga información sobre la compatibilidad con RHEL 8 y 9 con el conector" .

Compatibilidad con Podman 4.9.4 con todas las versiones de RHEL

Podman 4.9.4 ahora es compatible con todas las versiones compatibles de Red Hat Enterprise Linux. Anteriormente, la versión 4.9.4 solo era compatible con RHEL 8.10.

La lista actualizada de versiones compatibles de Podman incluye 4.6.1 y 4.9.4 con hosts Red Hat Enterprise Linux.

Podman es necesario para los hosts RHEL a partir de la versión 3.9.40 del Conector.

"Obtenga información sobre la compatibilidad con RHEL 8 y 9 con el conector" .

Permisos de AWS y Azure actualizados

Actualizamos las políticas de AWS y Azure para el Conector para eliminar los permisos que ya no son necesarios. Los permisos estaban relacionados con el almacenamiento en caché de borde de BlueXP y el descubrimiento y la administración de clústeres de Kubernetes, que ya no son compatibles a partir de agosto de 2024.

- "Conozca qué cambió en la política de AWS" .
- "Descubra qué cambió en la política de Azure" .

22 de agosto de 2024

Parche del conector 3.9.43

Actualizamos el conector para admitir la versión 9.15.1 de Cloud Volumes ONTAP .

El soporte para esta versión incluye una actualización de la política del conector para Azure. La política ahora incluye los siguientes permisos:

```
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/delete"
```

Estos permisos son necesarios para que Cloud Volumes ONTAP admita conjuntos de escala de máquinas virtuales. Si tiene conectores existentes y desea utilizar esta nueva característica, deberá agregar estos permisos a los roles personalizados que están asociados con sus credenciales de Azure.

- "Obtenga más información sobre la versión 9.15.1 de Cloud Volumes ONTAP"
- "Ver los permisos de Azure para el conector" .

8 de agosto de 2024

Conector 3.9.43

Esta versión incluye pequeñas mejoras y correcciones de errores.

La versión 3.9.43 está disponible para el modo estándar y el modo restringido.

Requisitos de CPU y RAM actualizados

Para proporcionar una mayor confiabilidad y mejorar el rendimiento de BlueXP y el Conector, ahora necesitamos CPU y RAM adicionales para la máquina virtual del Conector:

- CPU: 8 núcleos u 8 vCPU (el requisito anterior era 4)
- RAM: 32 GB (el requisito anterior era 14 GB)

Como resultado de este cambio, el tipo de instancia de VM predeterminado al implementar el Conector desde BlueXP o desde el mercado del proveedor de la nube es el siguiente:

- AWS: t3.2xgrande
- Azure: Estándar_D8s_v3
- Google Cloud: n2-estándar-8

Los requisitos actualizados de CPU y RAM se aplican a todos los conectores nuevos. Para los conectores existentes, se recomienda aumentar la CPU y la RAM para proporcionar un mejor rendimiento y confiabilidad.

Compatibilidad con Podman 4.9.4 con RHEL 8.10

La versión 4.9.4 de Podman ahora es compatible al instalar el conector en un host Red Hat Enterprise Linux 8.10.

Validación de usuarios para la federación de identidades

Si utiliza la federación de identidad con BlueXP, cada usuario que inicie sesión en BlueXP por primera vez deberá completar un formulario rápido para validar su identidad.

31 de julio de 2024

Lanzamiento del modo privado (3.9.42)

Ya está disponible para descargar una nueva versión del modo privado desde el sitio de soporte de NetApp .

Compatibilidad con RHEL 8 y 9

Esta versión incluye soporte para instalar el Conector en un host Red Hat Enterprise Linux 8 o 9 cuando se utiliza BlueXP en modo privado. Se admiten las siguientes versiones de RHEL:

- 8.6 a 8.10
- 9.1 a 9.3

Se requiere Podman como herramienta de orquestación de contenedores para estos sistemas operativos.

Debe conocer los requisitos de Podman, las limitaciones conocidas, un resumen de la compatibilidad del sistema operativo, qué hacer si tiene un host RHEL 7, cómo comenzar y más.

"Obtenga información sobre la compatibilidad con RHEL 8 y 9 con el conector" .

Versiones incluidas en esta versión

Esta versión incluye las siguientes versiones de los servicios BlueXP que son compatibles con el modo privado.

Servicio	Versión incluida
Conector	3.9.42
Copia de seguridad y recuperación	18 de julio de 2024
Clasificación	1 de julio de 2024 (versión 1.33)
Administración de Cloud Volumes ONTAP	10 de junio de 2024
Monedero digital	30 de julio de 2023
Gestión de clústeres ONTAP locales	30 de julio de 2023
Replicación	18 de septiembre de 2022

Para obtener más información sobre lo que se incluye en las versiones de estos servicios de BlueXP , consulte las notas de la versión de cada servicio de BlueXP .

- "Conozca el modo privado"
- "Aprenda cómo comenzar a usar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"
- "Descubra las novedades sobre la BlueXP backup and recovery"
- "Descubra las novedades de la BlueXP classification"
- "Descubra las novedades sobre la administración de Cloud Volumes ONTAP en BlueXP"

15 de julio de 2024

Compatibilidad con RHEL 8.10

BlueXP ahora admite la instalación del Conector en un host Red Hat Enterprise Linux 8.10 cuando se utiliza el modo estándar o el modo restringido.

El soporte para RHEL 8.10 comienza con la versión 3.9.40 del Conector.

"Obtenga información sobre la compatibilidad con RHEL 8 y 9 con el conector" .

8 de julio de 2024

Conector 3.9.42

Esta versión incluye mejoras menores, correcciones de errores y soporte para el Conector en la región AWS Canadá Oeste (Calgary).

La versión 3.9.42 está disponible para el modo estándar y el modo restringido.

Requisitos actualizados de Docker Engine

Cuando el conector está instalado en un host Ubuntu, la versión mínima compatible de Docker Engine ahora es 23.0.6. Anteriormente era 19.3.1.

La versión máxima compatible sigue siendo 25.0.5.

"Ver requisitos de host del conector" .

Ahora se requiere verificación de correo electrónico

Los nuevos usuarios que se registren en BlueXP ahora deberán verificar su dirección de correo electrónico antes de poder iniciar sesión.

12 de junio de 2024

Conector 3.9.41

Esta versión del conector BlueXP incluye pequeñas mejoras de seguridad y correcciones de errores.

La versión 3.9.41 está disponible para el modo estándar y el modo restringido.

Fin del soporte para RHEL 7 y CentOS 7

El 30 de junio de 2024, RHEL 7 alcanzó el final del mantenimiento (EOM), mientras que CentOS 7 alcanzó el final de su vida útil (EOL). NetApp suspendió el soporte para agentes en estas distribuciones de Linux el 30 de junio de 2024.

"Red Hat: Qué debe saber sobre el fin del mantenimiento de Red Hat Enterprise Linux 7"

Si tiene un agente existente ejecutándose en RHEL 7 o CentOS 7, NetApp no admite la actualización ni la conversión del sistema operativo a RHEL 8 o 9. Debe crear un nuevo agente en un sistema operativo compatible.

1. Configurar un host RHEL 8 o 9.
2. Instalar Podman.
3. Instalar un *nuevo* agente.
4. Configure el agente para descubrir los sistemas que administraba el agente anterior.
5. Redescubrir los sistemas.

   Consulte las siguientes páginas para redescubrir sus sistemas después de implementar un nuevo agente de consola.

   - "Agregar sistemas Cloud Volumes ONTAP existentes"
   - "Descubra los clústeres ONTAP locales"
   - "Crear o descubrir un sistema FSx para ONTAP"
   - "Crear un sistema de Azure NetApp Files"
   - "Descubra los sistemas de la Serie E"
   - "Descubra los sistemas StorageGRID"

4 de junio de 2024

Lanzamiento del modo privado (3.9.40)

Ya está disponible para descargar una nueva versión del modo privado desde el sitio de soporte de NetApp . Esta versión incluye las siguientes versiones de los servicios BlueXP que son compatibles con el modo privado.

Tenga en cuenta que esta versión de modo privado *no* incluye soporte para el Conector con Red Hat Enterprise Linux 8 y 9.

Servicio	Versión incluida
Conector	3.9.40
Copia de seguridad y recuperación	17 de mayo de 2024
Clasificación	15 de mayo de 2024 (versión 1.31)
Administración de Cloud Volumes ONTAP	17 de mayo de 2024
Monedero digital	30 de julio de 2023
Gestión de clústeres ONTAP locales	30 de julio de 2023
Replicación	18 de septiembre de 2022

Para obtener más información sobre lo que se incluye en las versiones de estos servicios de BlueXP , consulte las notas de la versión de cada servicio de BlueXP .

- "Conozca el modo privado"
- "Aprenda cómo comenzar a usar BlueXP en modo privado"
- "Aprenda a actualizar el conector cuando use el modo privado"
- "Descubra las novedades sobre la BlueXP backup and recovery"

- "Descubra las novedades de la BlueXP classification"
- "Descubra las novedades sobre la administración de Cloud Volumes ONTAP en BlueXP"

17 de mayo de 2024

Conector 3.9.40

Esta versión del conector BlueXP incluye soporte para sistemas operativos adicionales, mejoras de seguridad menores y correcciones de errores.

En este momento, la versión 3.9.40 está disponible para el modo estándar y el modo restringido.

Compatibilidad con RHEL 8 y 9

El conector ahora es compatible con hosts que ejecutan las siguientes versiones de Red Hat Enterprise Linux con *nuevas* instalaciones del conector cuando se utiliza BlueXP en modo estándar o modo restringido:

- 8.6 a 8.9
- 9.1 a 9.3

Se requiere Podman como herramienta de orquestación de contenedores para estos sistemas operativos.

Debe conocer los requisitos de Podman, las limitaciones conocidas, un resumen de la compatibilidad del sistema operativo, qué hacer si tiene un host RHEL 7, cómo comenzar y más.

"Obtenga información sobre la compatibilidad con RHEL 8 y 9 con el conector" .

Fin del soporte para RHEL 7 y CentOS 7

El 30 de junio de 2024, RHEL 7 llegará al final del mantenimiento (EOM), mientras que CentOS 7 llegará al final de su vida útil (EOL). NetApp continuará brindando soporte al Conector en estas distribuciones de Linux hasta el 30 de junio de 2024.

"Descubra qué hacer si tiene un conector existente ejecutándose en RHEL 7 o CentOS 7" .

Actualización de permisos de AWS

En la versión 3.9.38, actualizamos la política del conector para AWS para incluir el permiso "ec2:DescribeAvailabilityZones". Este permiso ahora es necesario para admitir zonas locales de AWS con Cloud Volumes ONTAP.

- "Ver los permisos de AWS para el conector" .
- "Obtenga más información sobre el soporte para las zonas locales de AWS"

Limitaciones conocidas de NetApp Console

Las limitaciones conocidas identifican plataformas, dispositivos o funciones que no son compatibles con esta versión del producto o que no interoperan correctamente con él. Revise estas limitaciones cuidadosamente.

Estas limitaciones son específicas de la configuración de la NetApp Console : el agente, la plataforma de software como servicio (SaaS) y más.

Limitaciones del agente de consola

Posible conflicto con direcciones IP en el rango 172

La NetApp Console implementa un agente con dos interfaces que tienen direcciones IP en los rangos 172.17.0.0/16 y 172.18.0.0/16.

Si su red tiene una subred configurada con cualquiera de estos rangos, es posible que experimente fallas de conectividad desde la consola. Por ejemplo, la detección de clústeres ONTAP locales en la consola podría fallar.

Ver artículo de la base de conocimientos"Conflicto de IP del agente con la red existente" para obtener instrucciones sobre cómo cambiar la dirección IP de las interfaces del agente.

El descifrado SSL es compatible solo con Cloud Volumes ONTAP

Los servidores proxy transparentes son compatibles solo con agentes asociados con Cloud Volumes ONTAP. No puedes usar un proxy transparente para un agente si se usa con otros servicios de datos de NetApp. Si usas servicios de datos de NetApp con Cloud Volumes ONTAP, crea un agente dedicado para Cloud Volumes ONTAP donde puedas usar un servidor proxy transparente.

Para mayor seguridad, tienes la opción de"Instalar un certificado HTTPS firmado por una autoridad de certificación (CA)" .

Página en blanco al cargar la interfaz de usuario local

Si carga la consola basada en web que se ejecuta en un agente, es posible que a veces la interfaz no se muestre y solo aparezca una página en blanco.

Este problema está relacionado con un problema de almacenamiento en caché. La solución alternativa es utilizar una sesión de navegador web privada o de incógnito.

Los hosts Linux compartidos no son compatibles

El agente no es compatible con una máquina virtual compartida con otras aplicaciones. La VM debe estar dedicada al software del agente.

Agentes y extensiones de terceros

Los agentes de terceros o las extensiones de máquina virtual no son compatibles con la máquina virtual del agente.

Empezar

Aprenda los conceptos básicos

Obtenga más información sobre la NetApp Console

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

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

Gestión centralizada del almacenamiento

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

Almacenamiento en la nube y local compatible

Puede administrar los siguientes tipos de almacenamiento desde la consola:

Soluciones de almacenamiento en la nube

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

Almacenamiento de objetos y flash local

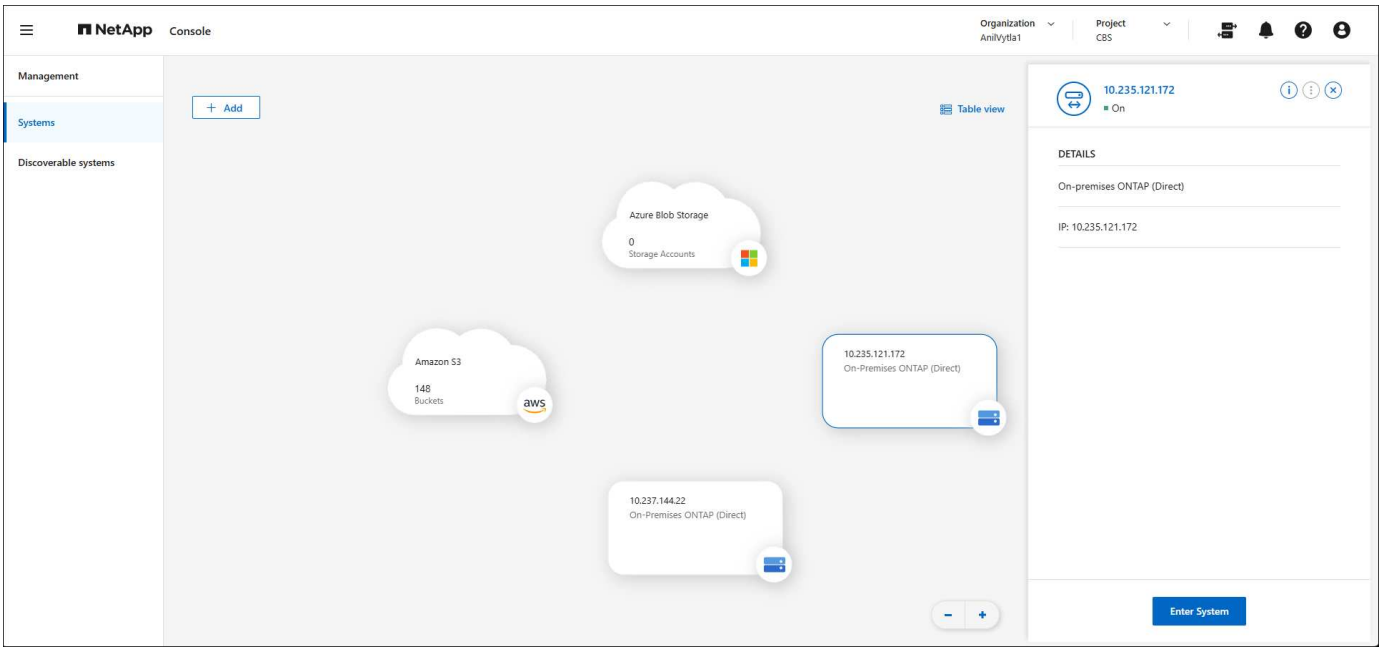
- Sistemas de la serie E
- Clústeres ONTAP
- Sistemas StorageGRID

Almacenamiento de objetos en la nube

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

Gestión de almacenamiento

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



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

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

Alertas de almacenamiento

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

Centro de automatización

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

NetApp Backup and Recovery

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

NetApp Data Classification

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

NetApp Copy and Sync

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

Asesor digital de NetApp (Active IQ)

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

Licenses and subscriptions

Administre y monitoree sus licencias y suscripciones.

NetApp Disaster Recovery

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

Planificación del ciclo de vida

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

NetApp Ransomware Resilience

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

NetApp Replication

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

Actualizaciones de software

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

Panel de sostenibilidad

Analice la sostenibilidad de sus sistemas de almacenamiento.

NetApp Cloud Tiering

Amplíe su almacenamiento ONTAP local a la nube.

NetApp Volume Caching

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

Cargas de trabajo de NetApp

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

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

Proveedores de nube compatibles

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

Costo

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

Cómo funciona la NetApp Console

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

Software como servicio

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

Gestión de identidad y acceso (IAM)

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

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

Agentes de consola

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

"Obtenga más información sobre los agentes de consola" .

Implementación de SaaS versus nube soberana

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

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

"Obtenga más información sobre los modos de implementación" .

Certificación SOC 2 Tipo 2

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

"Ver los informes SOC 2 de NetApp"

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

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

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

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

Descripción general

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

Modo estándar

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

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

Modo restringido

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

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

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

Modo privado de BlueXP (solo interfaz heredada de BlueXP)

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

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

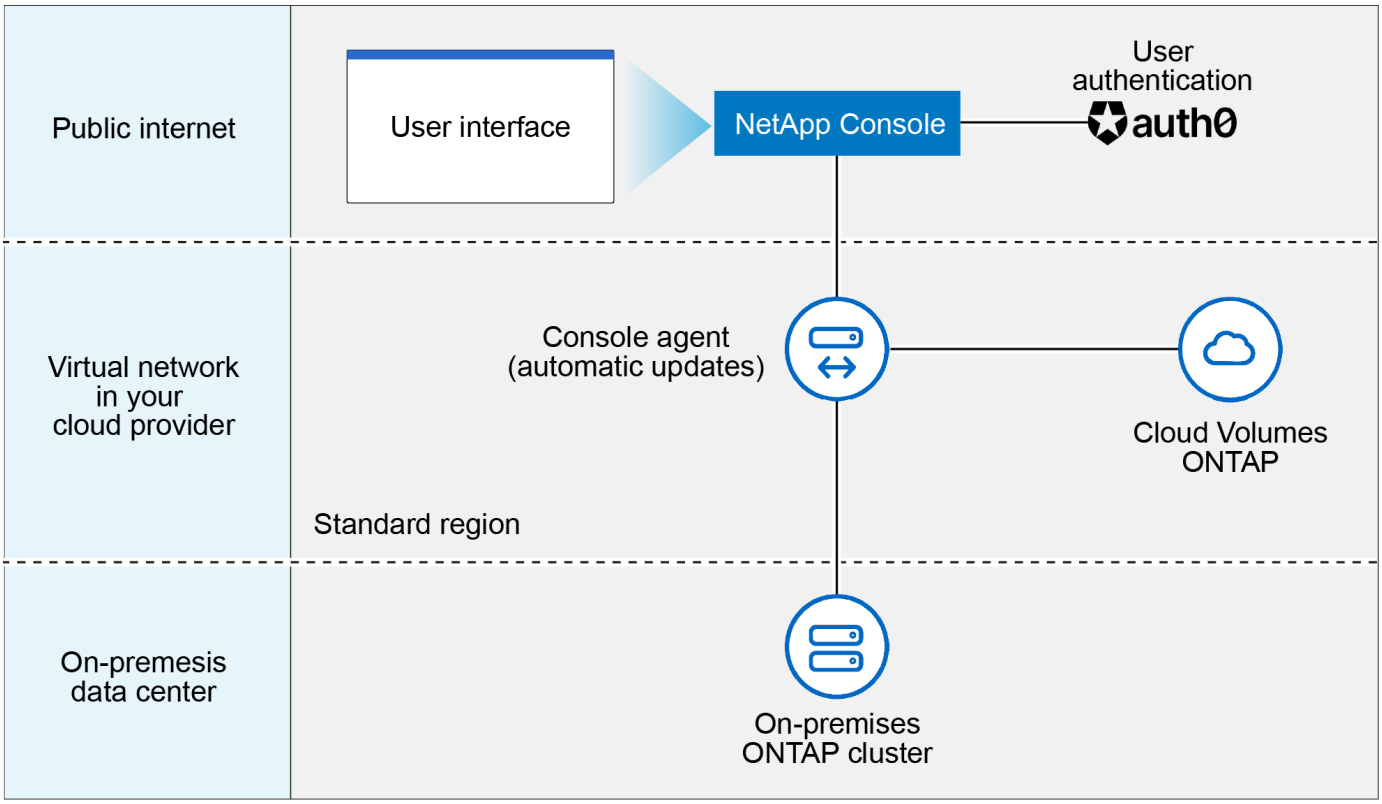
	Modo estándar	Modo restringido
¿Se requiere conexión a la capa SaaS de la NetApp Console ?	Sí	Solo salida
¿Es necesario conectarse a su proveedor de nube?	Sí	Sí, dentro de la región
Instalación del agente de consola	Desde la consola, el mercado en la nube o la instalación manual	Mercado en la nube o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

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

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

Modo estándar

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



La consola funciona de la siguiente manera en modo estándar:

Comunicación saliente

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

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

Ubicación compatible con un agente

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

Instalación del agente de consola

Puede instalar un agente utilizando uno de los siguientes métodos:

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

Actualizaciones del agente de consola

NetApp actualiza automáticamente su agente mensualmente.

Acceso a la interfaz de usuario

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

Punto final de API

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

Autenticación

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

Servicios de datos compatibles

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

Opciones de licencia admitidas

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

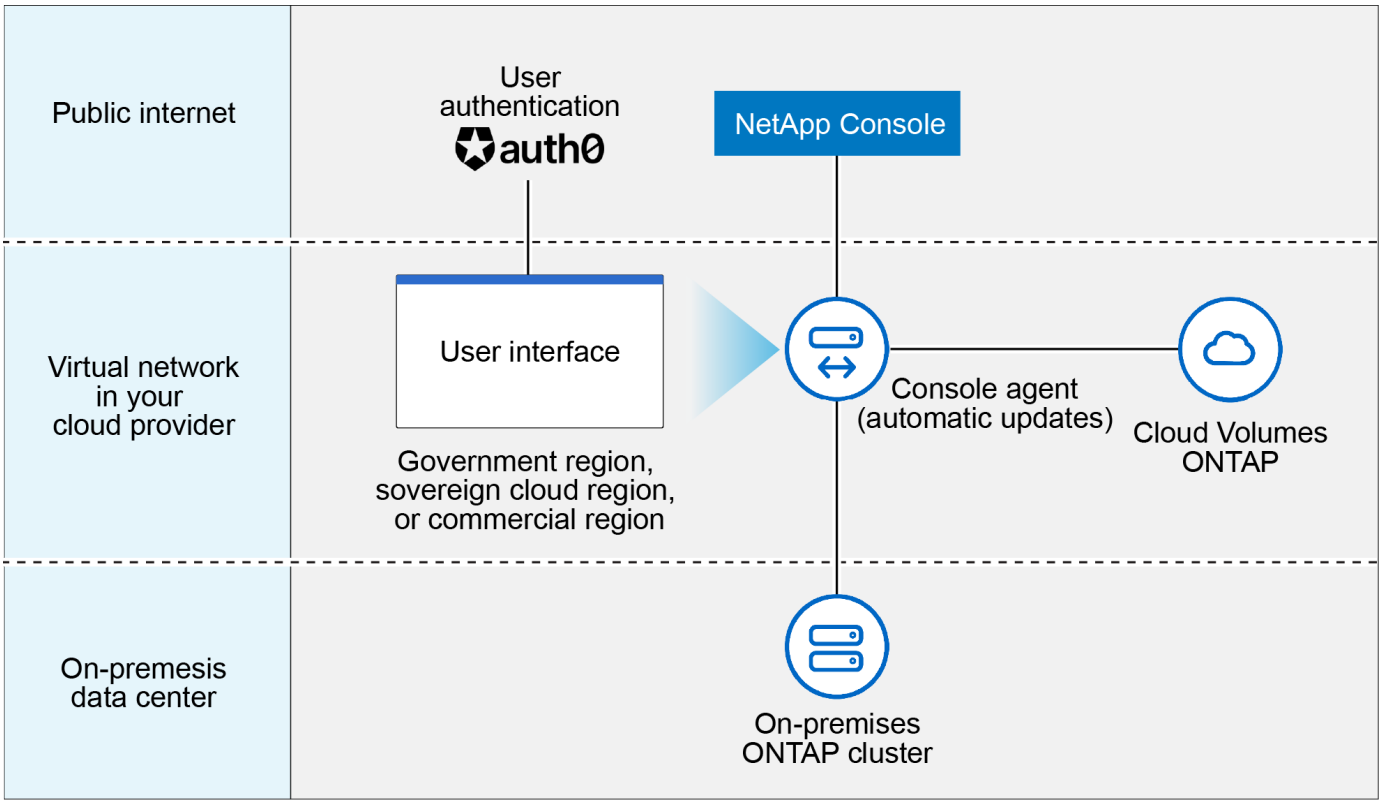
Cómo empezar a utilizar el modo estándar

Ir a la "NetApp Console" y regístrate.

"Aprenda cómo comenzar a utilizar el modo estándar" .

Modo restringido

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



La consola funciona de la siguiente manera en modo restringido:

Comunicación saliente

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

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

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

Ubicación compatible con un agente

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

Instalación del agente de consola

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

Actualizaciones del agente de consola

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

Acceso a la interfaz de usuario

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

Punto final de API

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

Autenticación

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

Servicios de datos y gestión de almacenamiento compatibles

Los siguientes servicios de almacenamiento y datos con modo restringido:

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

Opciones de licencia admitidas

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

- Suscripciones al Marketplace (contratos por hora y anuales)

  Tenga en cuenta lo siguiente:

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

- Trae tu propia bebida

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

Cómo empezar a utilizar el modo restringido

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

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

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

"Aprenda cómo comenzar a utilizar el modo restringido" .

Comparación de servicios y características

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

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

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

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

Administrar las credenciales NSS asociadas con la NetApp Console

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

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

Descripción general

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

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

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

- Registro de sistemas Cloud Volumes ONTAP de pago por uso

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

- Actualización del software Cloud Volumes ONTAP a la última versión

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

Agregar una cuenta NSS

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

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

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

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

Pasos

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

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

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

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

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

¿Que sigue?

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

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

Actualizar las credenciales de NSS

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

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

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

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

Pasos

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

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

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

Adjuntar un sistema a una cuenta NSS diferente

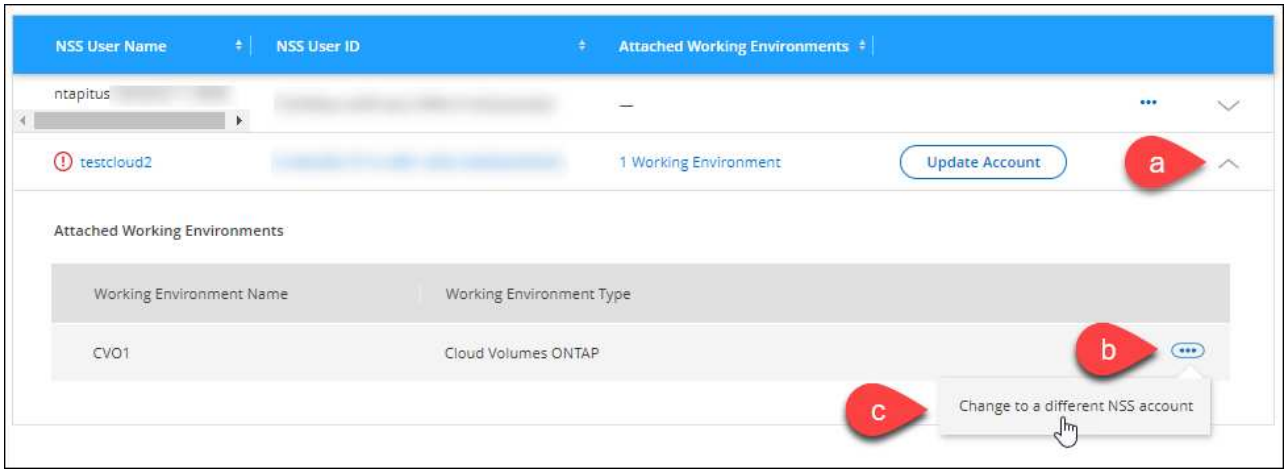
Si su organización tiene varias cuentas de sitio de soporte de NetApp , puede cambiar qué cuenta está asociada con un sistema Cloud Volumes ONTAP .

Primero debes haber asociado la cuenta con la Consola.

Pasos

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

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



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

Mostrar la dirección de correo electrónico de una cuenta NSS

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

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

Pasos

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

Eliminar una cuenta NSS

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

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

Pasos

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

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

Obtenga más información sobre los agentes de la NetApp Console

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

Un agente de consola le permite:

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

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

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

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

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

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

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

adecuado.

Los agentes de consola deben estar operativos en todo momento

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

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

Ubicaciones compatibles

Puede instalar agentes en las siguientes ubicaciones:

- Servicios web de Amazon
- Microsoft Azure

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

- Google Cloud

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

- En sus instalaciones

Comunicación con proveedores de la nube

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

Modo restringido

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

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

Cómo instalar un agente de consola

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

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

Permisos del proveedor de la nube

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

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

Para saber cómo configurar permisos, consulte lo siguiente:

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

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

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

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

Actualizaciones de agente

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

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

Mantenimiento del sistema operativo y de máquinas virtuales

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

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

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

El agente de consola debe estar operativo en todo momento .

Múltiples sistemas y agentes

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

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

A continuación se muestran algunos ejemplos de implementaciones de agentes:

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

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

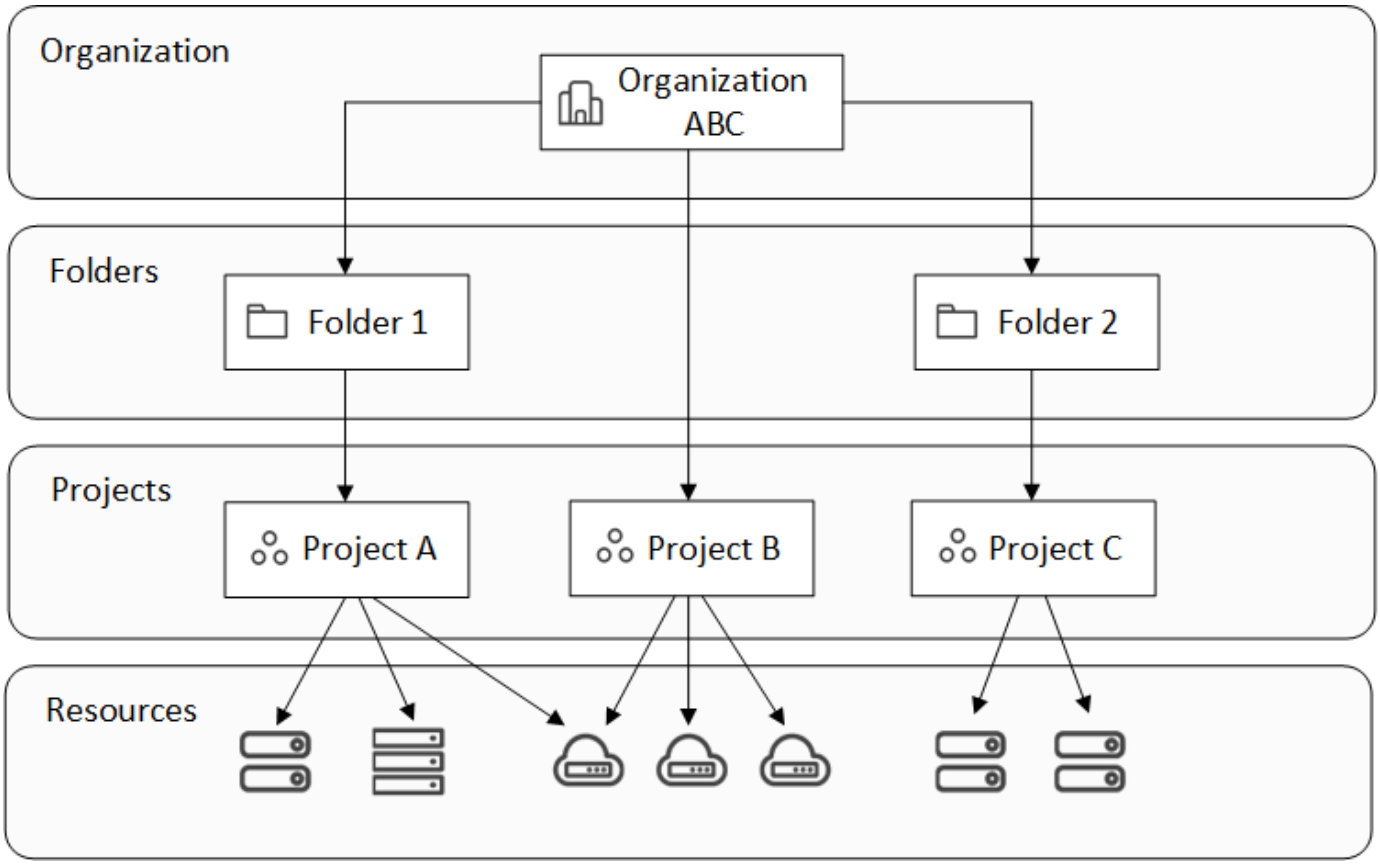
Utilice la gestión de identidad y acceso (IAM) de la consola de NetApp para organizar sus recursos de NetApp y controlar el acceso según la estructura de su negocio: por ubicación, departamento o proyecto.

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

Asigna roles de acceso a nivel de organización, carpeta o proyecto para que los usuarios tengan el acceso correcto a los recursos.

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

La siguiente imagen ilustra esta jerarquía en un nivel básico.



]

Componentes de gestión de identidad y acceso

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

Proyectos y carpetas dentro de su organización

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

Organización

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

Proyectos

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

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

"Aprenda cómo agregar proyectos a su organización."

Carpetas

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

"Aprenda cómo agregar carpetas a su organización."

Recursos

Un *recurso* es una entidad de la que la Console tiene conocimiento y que puede asignarse a un proyecto. *Recursos* incluyen sistemas de almacenamiento, suscripciones a Keystone, algunas cargas de trabajo de Backup and Recovery, así como agentes de la Console.

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

+

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

+

"Aprenda a asociar recursos a proyectos."

Sistemas de almacenamiento y suscripciones Keystone

Los sistemas de almacenamiento son los recursos principales que gestionas en NetApp Console. NetApp Console admite la gestión de sistemas de almacenamiento tanto locales como en la nube. Debes añadir un sistema de almacenamiento a un proyecto para que puedan acceder a él quienes estén asignados al proyecto.

Sistemas de almacenamiento

Los sistemas de almacenamiento se asocian automáticamente al proyecto donde se añaden, pero puedes asociarlos a otros proyectos o carpetas desde la página **Resources**. No puedes asociar sistemas de almacenamiento FSx para NetApp ONTAP a proyectos o carpetas, pero puedes verlos en la página **Systems** o desde Workloads.

Suscripciones a Keystone

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

Cargas de trabajo de Backup and Recovery (Oracle y Microsoft SQL Server)

Algunas cargas de trabajo de Backup and Recovery también se consideran recursos. Puedes asignar permisos a los usuarios para acceder a Backup and Recovery

Agentes de consola

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

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

"Aprenda a asociar agentes con proyectos."

Miembros y roles

Miembros

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

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

"Aprenda cómo agregar miembros a su organización."

Roles de acceso

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

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

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

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

"Obtenga más información sobre los roles de acceso" .

Ejemplos de estrategias de IAM

Estrategia de organización pequeña

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

Ejemplo: Corporación ABC (equipo de 5 personas)

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

Estrategia empresarial multirregional

Para organizaciones grandes con operaciones regionales y equipos especializados, implemente un enfoque

jerárquico con carpetas que representen límites geográficos o de unidades de negocios.

Ejemplo: Corporación XYZ (empresa multinacional)

- **Estructura:** Organización > Carpetas regionales (Norteamérica, Europa, Asia-Pacífico) > Carpetas de proyectos por región
- **Roles de plataforma:**
  - 1 **Administrador de la organización**: Supervisión global y gestión de políticas
  - 3 **Administradores de carpetas o proyectos**: Control regional (uno por región)
  - 1 **Administrador de la federación**: Integración del proveedor de identidad corporativa
- **Roles de almacenamiento por región:**
  - 9 **Administrador de almacenamiento**: descubre y administra sistemas de almacenamiento en regiones asignadas
  - 2 **Visor de almacenamiento**: Supervise los recursos de almacenamiento en todas las regiones
  - 1 **Especialista en salud del sistema**: Administra la salud del almacenamiento sin modificaciones del sistema
- **Roles de servicio de datos:**
  - **Administrador de copias de seguridad y recuperación**: por proyecto, según las responsabilidades de copia de seguridad
  - **Administrador de resiliencia ante ransomware**: Supervisión del equipo de seguridad en todos los proyectos
- **Estrategia del agente:** Agentes regionales asociados a proyectos geográficos apropiados
- **Beneficios:** Mayor seguridad mediante la segregación de roles, autonomía regional y cumplimiento de las regulaciones locales.

Estrategia de especialización departamental

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

Ejemplo: TechCorp (empresa tecnológica de tamaño mediano)

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

Próximos pasos con IAM en la NetApp Console

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

Comience a usar NetApp Console (Saas)

Flujo de trabajo de introducción (SaaS)

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

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

1 **"Preparar la red para usar la consola de NetApp"**

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

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

2 **"Regístrate y crea una organización"**

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

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

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

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

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

4 **Crear un agente de consola**

Las funciones de administración de almacenamiento avanzada y algunos servicios de datos de NetApp requieren que instale un agente de consola. El agente de la consola permite que la consola administre

recursos y procesos dentro de su entorno de nube híbrida.

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

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

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

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

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

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

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

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

Preparar el acceso a la red para la NetApp Console

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

Necesitará configurar el acceso a la red para lo siguiente:

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

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

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

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

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

Puntos finales	Objetivo
\ https://mysupport.netapp.com	Para obtener información de licencias y enviar mensajes de AutoSupport al soporte de NetApp .
\ https://signin.b2c.netapp.com	Para actualizar las credenciales del sitio de soporte de NetApp (NSS) o para agregar nuevas credenciales de NSS a la NetApp Console.
\ https://support.netapp.com	Para obtener información de licencias y enviar mensajes de AutoSupport al soporte de NetApp , así como para recibir actualizaciones de software para Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Proporcionar funciones y servicios dentro de la NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obtener imágenes para las actualizaciones del agente de consola. • Cuando se implementa un nuevo agente, la verificación de validación prueba la conectividad con los puntos finales actuales. Si utilizas"puntos finales anteriores" , la comprobación de validación falla. Para evitar este error, omita la comprobación de validación. Aunque los puntos finales anteriores aún son compatibles, NetApp recomienda actualizar las reglas de firewall a los puntos finales actuales lo antes posible. "Aprenda a actualizar su lista de puntos finales" . • Cuando actualice los puntos finales actuales en su firewall, sus agentes existentes continuarán funcionando.

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

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

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

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

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

Algunos servicios de datos de NetApp , así como Cloud Volumes ONTAP, requieren que el agente tenga acceso a Internet saliente adicional.

Puntos finales para Cloud Volumes ONTAP

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

Puntos finales para cargas de trabajo

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

Puntos finales	Objetivo
\ https://api.workloads.netapp.com	La consola basada en web se comunica con este punto final para interactuar con las API de Workload Factory para administrar y operar cargas de trabajo basadas en FSx para ONTAP.

Regístrese o inicie sesión en la NetApp Console

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

Regístrese en NetApp Console como administrador inicial de la organización

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

Pasos

1. Abra un navegador web y vaya a "NetApp Console"

2. Si tiene una cuenta del sitio de soporte de NetApp , ingrese la dirección de correo electrónico asociada a su cuenta directamente en la página **Iniciar sesión**.

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

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

      Sólo se permiten caracteres ingleses en el formulario de registro.

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

      Verifique su dirección de correo electrónico para completar el registro.

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

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

Próximos pasos

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

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

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

Pasos

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

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

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

      Sólo se permiten caracteres ingleses en el formulario de registro.

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

Verifique su dirección de correo electrónico para completar el registro.

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

Próximos pasos

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

Comience a utilizar el asistente de la NetApp Console

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

Roles necesarios para acceder al asistente de la consola

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

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

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

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

  "Aprenda cómo agregar una cuenta NSS".

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

  "Aprenda a instalar un agente de consola local."

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

  "Aprenda a agregar licencias y suscripciones".

- Revisar la información de los servicios de datos.

Introducción a NetApp Console (modo restringido)

Flujo de trabajo de introducción (modo restringido)

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

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

"Prepárese para el despliegue"

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

"Implementar el agente de consola"

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

"Suscríbete a los NetApp Intelligent Services (opcional)"

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

Prepárese para la implementación en modo restringido

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

Paso 1: Comprenda cómo funciona el modo restringido

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

Utilice la interfaz basada en navegador disponible localmente desde el agente de NetApp Console instalado. No se puede acceder a la NetApp Console desde la consola basada en web que se proporciona a través de la capa SaaS.

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

"Aprenda cómo funciona el modo restringido" .

Paso 2: Revisar las opciones de instalación

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

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

Paso 3: Revisar los requisitos del host

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

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

Host dedicado

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

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

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

  - `/var`:Debe haber 40 GiB de espacio disponibles

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

Tipo de instancia de AWS EC2

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

Tamaño de la máquina virtual de Azure

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

Tipo de máquina de Google Cloud

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

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

Hipervisor

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

Requisitos del sistema operativo y del contenedor

El agente de consola es compatible con los siguientes sistemas operativos cuando se utiliza la consola en

modo estándar o modo restringido. Se requiere una herramienta de orquestación de contenedores antes de instalar el agente.

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Red Hat Enterprise Linux		9,6 • Sólo versiones en idioma inglés. • El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación del agente.	4.0.0 o posterior con la consola en modo estándar o modo restringido	Podman versión 5.4.0 con podman-compose 1.5.0. Ver los requisitos de configuración de Podman .
Compatible con modo de aplicación o modo permisivo		9.1 a 9.4 • Sólo versiones en idioma inglés. • El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación del agente.	3.9.50 o posterior con la consola en modo estándar o modo restringido	Podman versión 4.9.4 con podman-compose 1.5.0. Ver los requisitos de configuración de Podman .

Sistema operativo	Versiones de sistema operativo compatibles	Versiones de agente compatibles	Herramienta de contenedor requerida	SELinux
Compatible con modo de aplicación o modo permisivo		8.6 a 8.10 • Sólo versiones en idioma inglés. • El host debe estar registrado en Red Hat Subscription Management. Si no está registrado, el host no puede acceder a los repositorios para actualizar el software de terceros requerido durante la instalación del agente.	3.9.50 o posterior con la consola en modo estándar o modo restringido	Podman versión 4.6.1 o 4.9.4 con podman-compose 1.0.6. Ver los requisitos de configuración de Podman .
Compatible con modo de aplicación o modo permisivo	Ubuntu		24,04 LTS	3.9.45 o posterior con la NetApp Console en modo estándar o modo restringido
Motor Docker 23.06 a 28.0.0.	No compatible		22,04 LTS	3.9.50 o posterior

Paso 4: Instalar Podman o Docker Engine

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

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

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

  Ver las versiones compatibles de Podman .

- Se requiere Docker Engine para Ubuntu.

  Ver las versiones compatibles de Docker Engine .

Ejemplo 1. Pasos

Podman

Siga estos pasos para instalar y configurar Podman:

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

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

Pasos

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

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

2. Instalar Podman.

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

   a. Para Red Hat Enterprise Linux 9,6:

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

   Donde <versión> es la versión compatible de Podman que estás instalando. Ver las versiones compatibles de Podman .

   b. Para Red Hat Enterprise Linux 9.1 a 9.4:

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

   Donde <versión> es la versión compatible de Podman que estás instalando. Ver las versiones compatibles de Podman .

   c. Para Red Hat Enterprise Linux 8:

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

   Donde <versión> es la versión compatible de Podman que estás instalando. Ver las versiones compatibles de Podman .

3. Habilite e inicie el servicio podman.socket.

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

4. Instalar python3.

```
sudo dnf install python3
```

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

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

6. Si utiliza Red Hat Enterprise 9:

   a. Instalar el paquete del repositorio EPEL.

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

   +

   a. Instalar el paquete podman-compose 1.5.0.

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

7. Si utiliza Red Hat Enterprise Linux 8:

   a. Instalar el paquete del repositorio EPEL.

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

   b. Instalar el paquete podman-compose 1.0.6.

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Reiniciar podman.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Motor Docker

Siga la documentación de Docker para instalar Docker Engine.

Pasos

1. "Ver instrucciones de instalación desde Docker"

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

2. Verifique que Docker esté habilitado y ejecutándose.

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

Paso 5: Preparar el acceso a la red

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

Conexiones a redes de destino

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

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

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

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

+

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

Acceso a Internet saliente para operaciones diarias

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

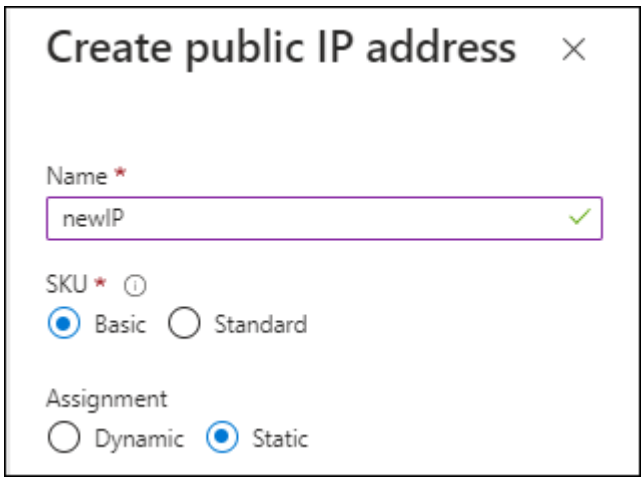
Puntos finales	Objetivo
Entornos AWS	Servicios de AWS (amazonaws.com): • Formación de nubes • Nube de cómputo elástica (EC2) • Gestión de identidad y acceso (IAM) • Servicio de gestión de claves (KMS) • Servicio de token de seguridad (STS) • Servicio de almacenamiento simple (S3)
Para administrar los recursos de AWS. El punto final depende de su región de AWS. "Consulte la documentación de AWS para obtener más detalles."	Amazon FsX para NetApp ONTAP: • api.workloads.netapp.com
La consola basada en web se comunica con este punto final para interactuar con las API de Workload Factory para administrar y operar FSx para cargas de trabajo basadas en ONTAP .	**Entornos Azure**
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Para administrar recursos en regiones públicas de Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Para administrar recursos en regiones de Azure Government.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Para administrar recursos en las regiones de Azure China.

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

Puntos finales	Objetivo
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Para obtener imágenes para las actualizaciones del agente de consola. • Cuando se implementa un nuevo agente, la verificación de validación prueba la conectividad con los puntos finales actuales. Si utilizas"puntos finales anteriores" , la comprobación de validación falla. Para evitar este error, omita la comprobación de validación. Aunque los puntos finales anteriores aún son compatibles, NetApp recomienda actualizar las reglas de firewall a los puntos finales actuales lo antes posible. "Aprenda a actualizar su lista de puntos finales" . • Cuando actualice los puntos finales actuales en su firewall, sus agentes existentes continuarán funcionando.

Dirección IP pública en Azure

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



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

"Documentación de Azure: SKU de IP pública"

Servidor proxy

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

- Dirección IP
- Cartas credenciales
- Certificado HTTPS

Puertos

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

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

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

Habilitar NTP

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

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

Paso 6: Preparar los permisos de la nube

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

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

Rol de AWS IAM

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

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

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

Pasos

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

Resultado

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

Clave de acceso de AWS

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

Pasos

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

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

   Para las regiones estándar, los permisos se distribuyen en dos políticas. Se requieren dos políticas debido a un límite máximo de tamaño de caracteres para las políticas administradas en AWS. "Obtenga más información sobre las políticas de IAM para el agente de consola" .
3. Adjuntar las políticas a un usuario de IAM.
   - "Documentación de AWS: Creación de roles de IAM"
   - "Documentación de AWS: Cómo agregar y eliminar políticas de IAM"

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

Rol de Azure

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

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

Pasos

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

   "Documentación de Microsoft Azure: Configurar identidades administradas para recursos de Azure en una máquina virtual mediante el portal de Azure"

2. Copiar el contenido del"Permisos de roles personalizados para el Conector" y guardarlos en un archivo JSON.
3. Modifique el archivo JSON agregando identificadores de suscripción de Azure al ámbito asignable.

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

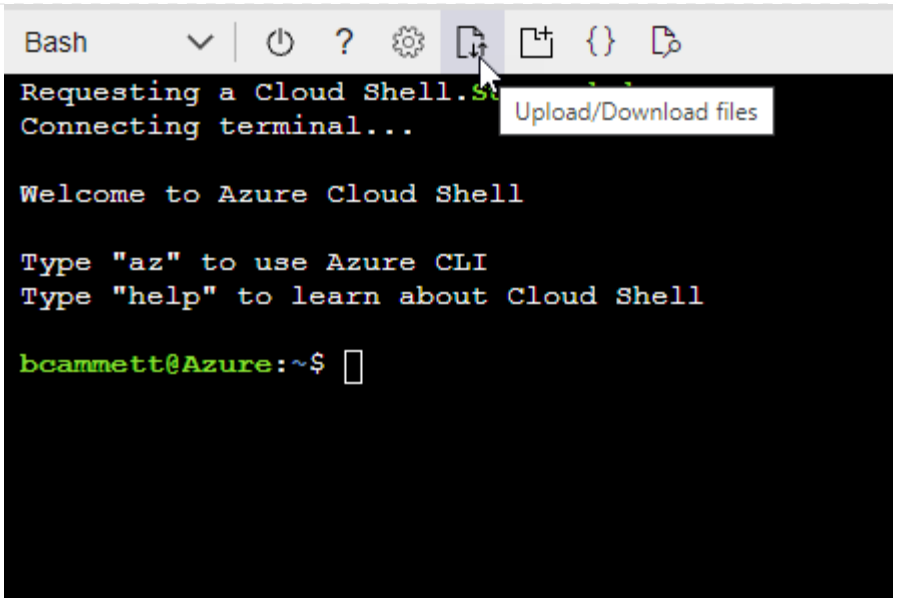
   Ejemplo

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

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

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

   a. Comenzar "Azure Cloud Shell" y elija el entorno Bash.
   b. Sube el archivo JSON.



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

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

entidad de servicio de Azure

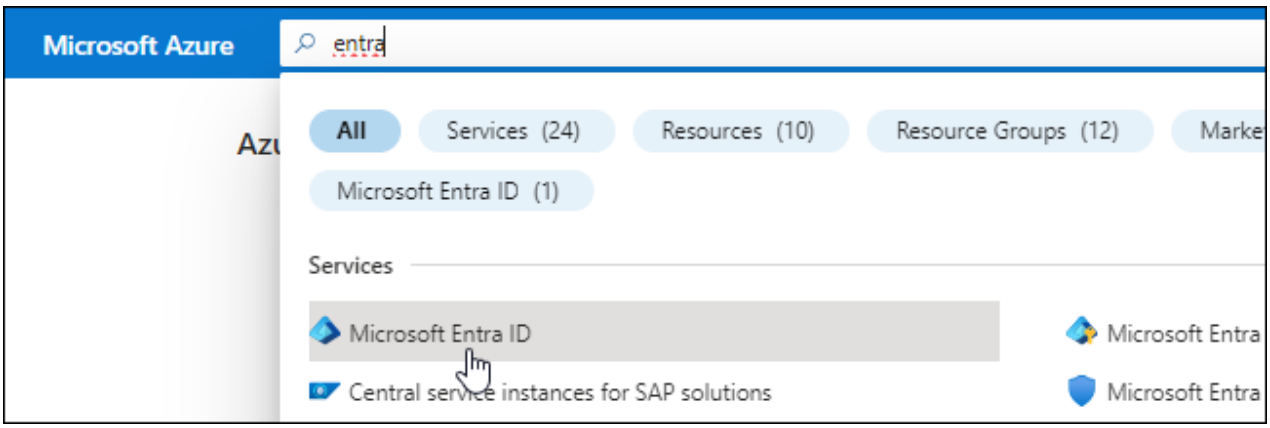
Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita la consola. Debe proporcionar a la consola estas credenciales después de instalar el agente de la consola.

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

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

   Para más detalles, consulte "Documentación de Microsoft Azure: Permisos necesarios"

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



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

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

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

Asignar la aplicación a un rol

1. Crear un rol personalizado:

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

   a. Copiar el contenido del"Permisos de roles personalizados para el agente de la consola" y guardarlos en un archivo JSON.

   b. Modifique el archivo JSON agregando identificadores de suscripción de Azure al ámbito asignable.

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

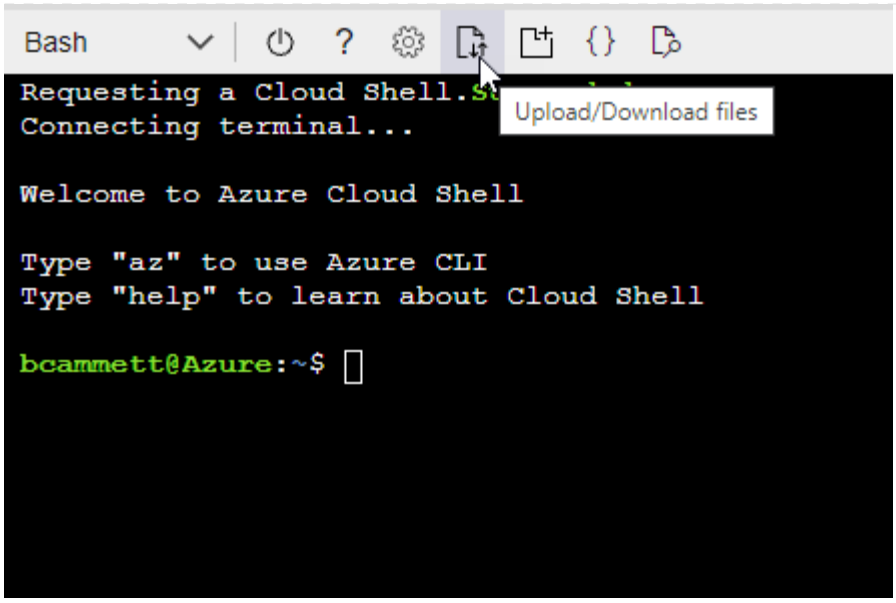
      Ejemplo

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

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

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

      - Comenzar "Azure Cloud Shell" y elija el entorno Bash.
      - Sube el archivo JSON.



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

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

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

2. Asignar la aplicación al rol:

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

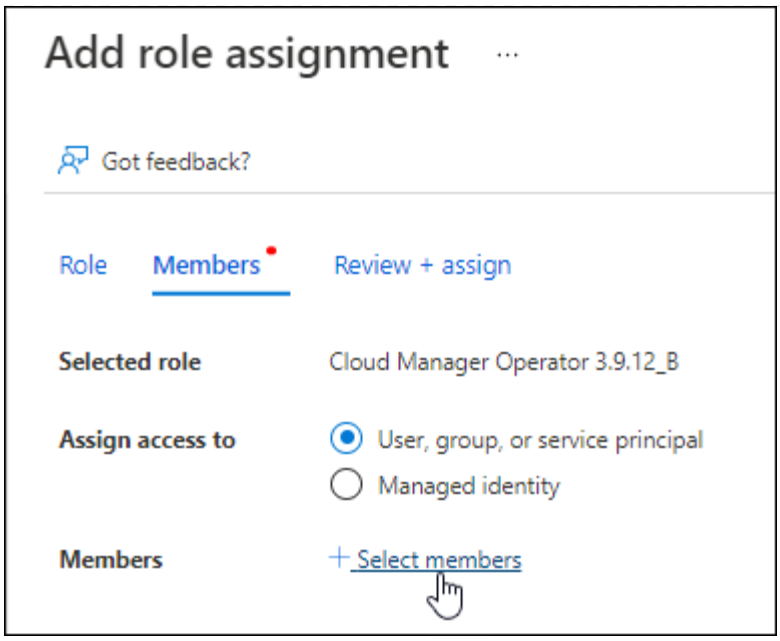
   b. Seleccione la suscripción.

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

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

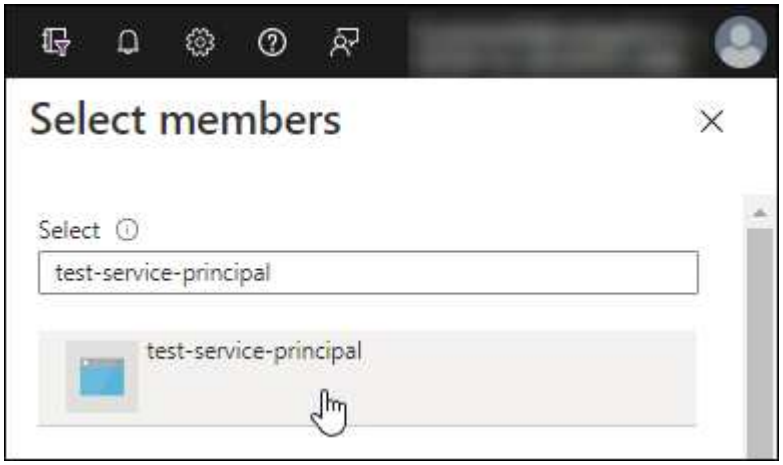
   e. En la pestaña **Miembros**, complete los siguientes pasos:

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



- Busque el nombre de la aplicación.

  He aquí un ejemplo:



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

f. Seleccione **Revisar + asignar**.

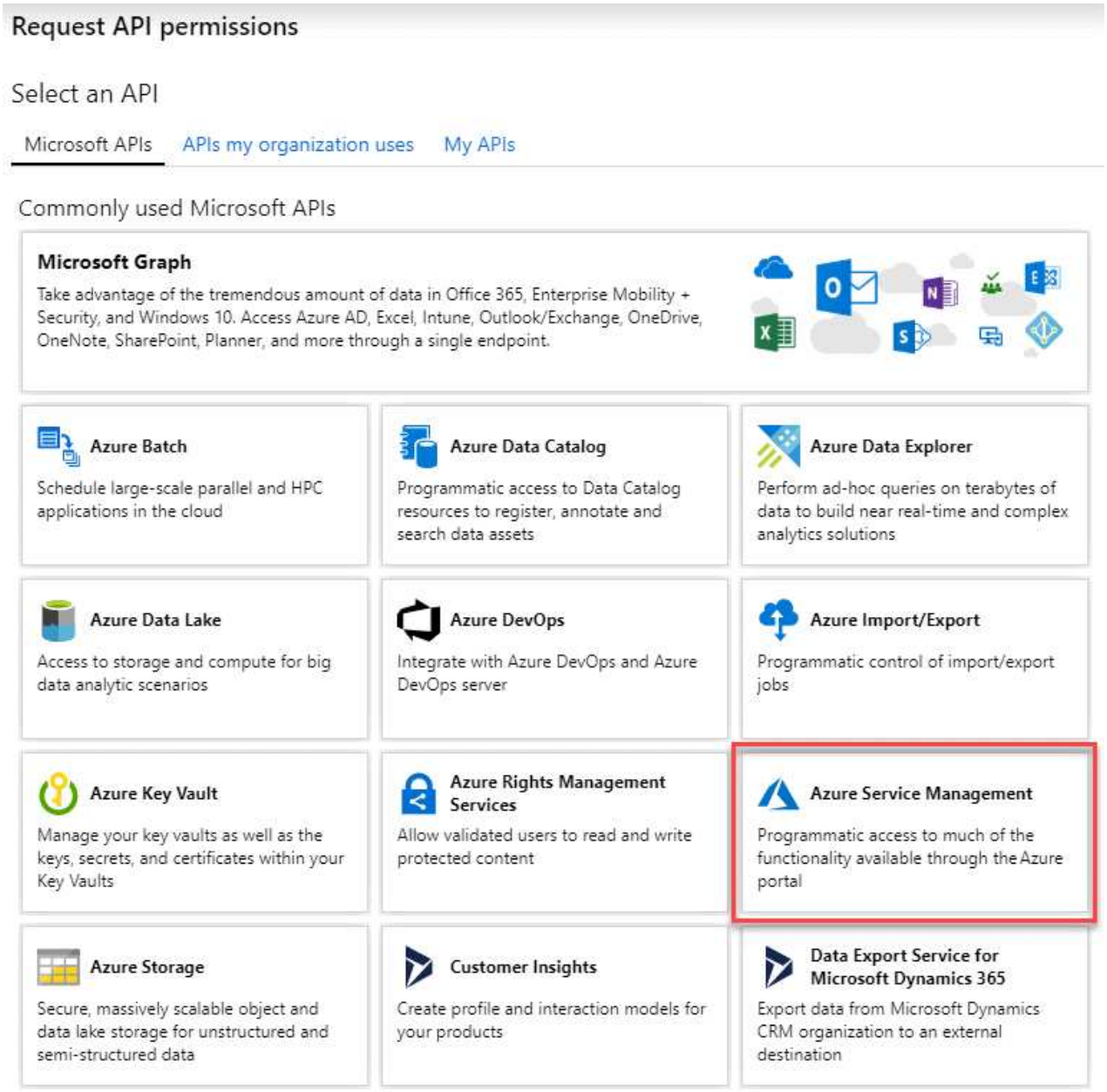
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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

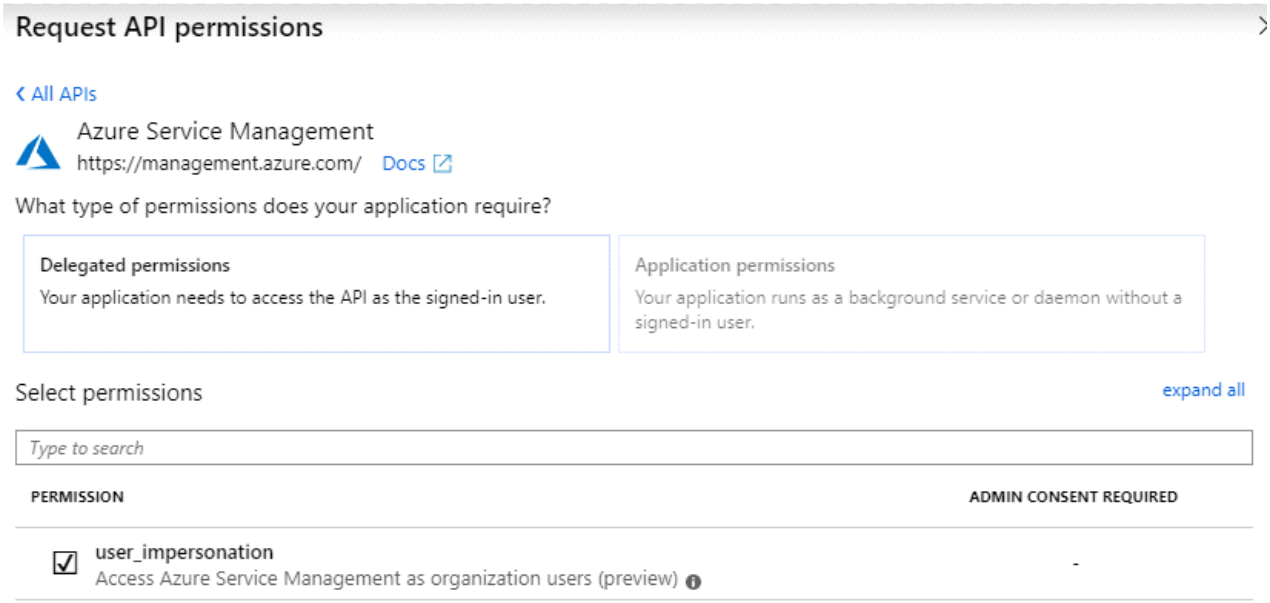
Agregar permisos de la API de administración de servicios de Windows Azure

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

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

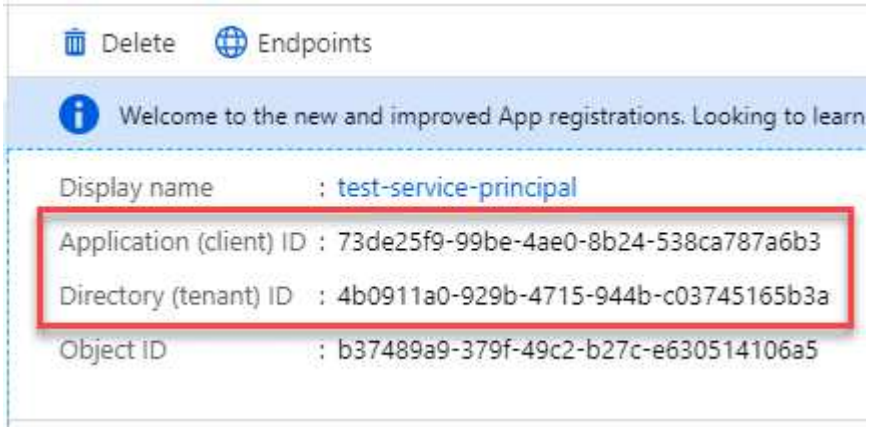


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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

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



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

Crear un secreto de cliente

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

Resultado

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

Cuenta de servicio de Google Cloud

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

Pasos

1. Crear un rol personalizado en Google Cloud:

   a. Cree un archivo YAML que incluya los permisos definidos en el"Política del agente de consola para Google Cloud" .

   b. Desde Google Cloud, activa Cloud Shell.

   c. Cargue el archivo YAML que incluye los permisos necesarios para el agente de consola.

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

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

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

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

2. Crear una cuenta de servicio en Google Cloud:

   a. Desde el servicio IAM y administración, seleccione **Cuentas de servicio > Crear cuenta de servicio**.

   b. Ingrese los detalles de la cuenta de servicio y seleccione **Crear y continuar**.

   c. Seleccione el rol que acaba de crear.

   d. Complete los pasos restantes para crear el rol.

      "Documentación de Google Cloud: Creación de una cuenta de servicio"

Paso 7: Habilitar las API de Google Cloud

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

Paso

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

Implementar el agente de consola en modo restringido

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

Paso 1: Instalar el agente de la consola

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

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

Mercado comercial de AWS

Antes de empezar

Tenga lo siguiente:

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

  "Obtenga más información sobre los requisitos de red"

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

  "Aprenda a configurar los permisos de AWS"

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

  "Requisitos del agente de revisión".

- Un par de claves para la instancia EC2.

Pasos

1. Ir a la "Listado de agentes de la NetApp Console en AWS Marketplace"
2. En la página de Marketplace, seleccione **Continuar con la suscripción**.
3. Para suscribirse al software, seleccione **Aceptar términos**.

   El proceso de suscripción puede tardar unos minutos.

4. Una vez completado el proceso de suscripción, seleccione **Continuar a la configuración**.
5. En la página **Configurar este software**, asegúrese de haber seleccionado la región correcta y luego seleccione **Continuar con el inicio**.
6. En la página **Iniciar este software**, en **Elegir acción**, seleccione **Iniciar a través de EC2** y luego seleccione **Iniciar**.

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

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

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

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

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

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

    - **Detalles avanzados**: en **Perfil de instancia de IAM**, elija el rol de IAM que incluye los permisos necesarios para el agente de consola.
    - **Resumen**: Revise el resumen y seleccione **Iniciar instancia**.

Resultado

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

¿Que sigue?

Configurar la NetApp Console.

Mercado gubernamental de AWS

Antes de empezar

Tenga lo siguiente:

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

  "Obtenga más información sobre los requisitos de red"

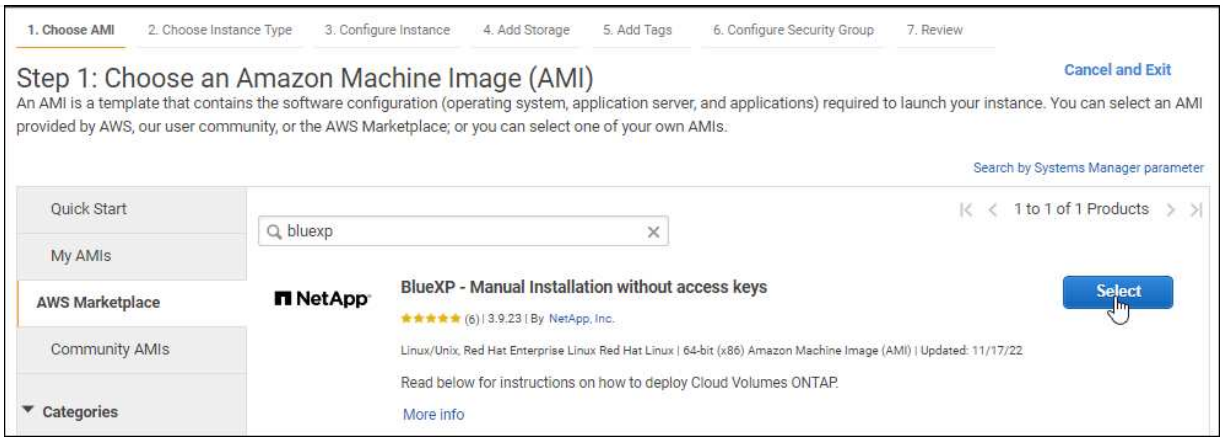
- Una función de IAM con una política adjunta que incluye los permisos necesarios para el agente de la consola.

  "Aprenda a configurar los permisos de AWS"

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

Pasos

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



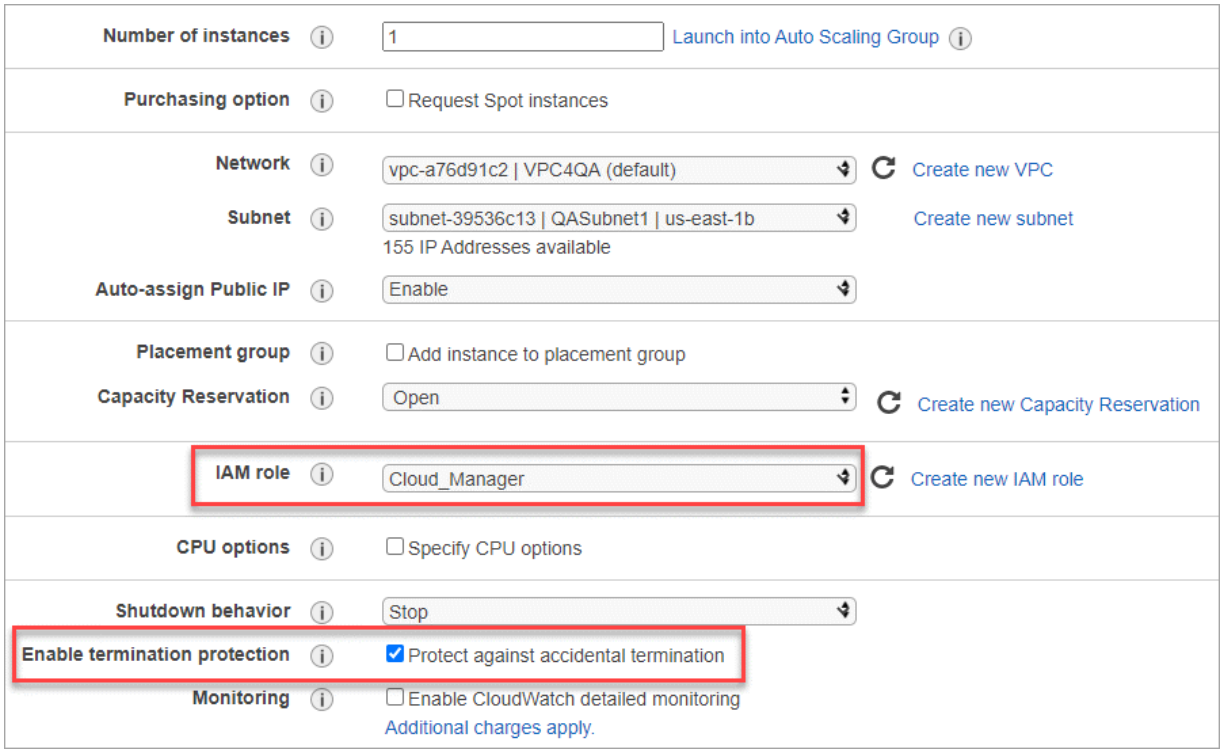
d. Seleccione **Continuar**.

2. Siga las instrucciones para configurar e iniciar la instancia:

   - **Elija un tipo de instancia**: según la disponibilidad de la región, elija uno de los tipos de instancia admitidos (se recomienda t3.2xlarge).

     "Revisar los requisitos de la instancia" .

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



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

Resultado

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

¿Que sigue?

Configurar la consola.

Mercado de Azure Gov

Antes de empezar

Debes tener lo siguiente:

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

  "Obtenga más información sobre los requisitos de red"

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

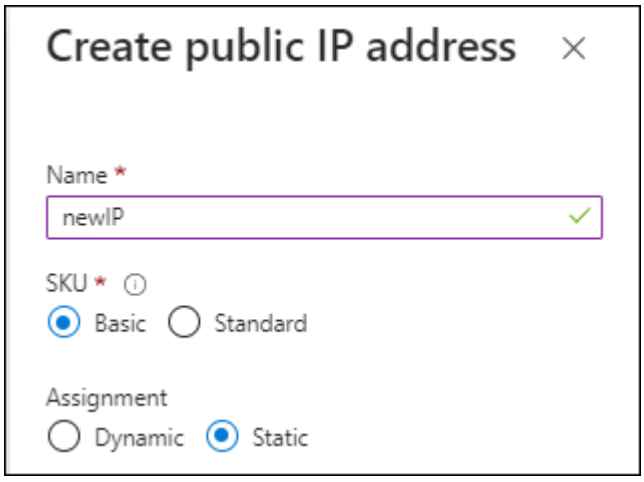
  "Aprenda a configurar los permisos de Azure"

Pasos

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

   Tenga en cuenta lo siguiente al configurar la máquina virtual:

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



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

alcanzar la dirección IP privada, la consola no funciona.

"Documentación de Azure: SKU de IP pública"

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

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

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

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

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

Resultado

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

¿Que sigue?

Configurar la NetApp Console.

Instalación manual (se debe usar para Google Cloud)

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

Antes de empezar

Debes tener lo siguiente:

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

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

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

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

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

Acerca de esta tarea

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

Pasos

1. Si las variables del sistema *http_proxy* o *https_proxy* están configuradas en el host, elimínelas:

   ```
   unset http_proxy
   unset https_proxy
   ```

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

2. Descargue el software del agente de consola y luego cópielo al host Linux. Puede descargarlo desde la NetApp Console o desde el sitio de soporte de NetApp .
   - NetApp Console: vaya a **Agentes > Administración > Implementar agente > Local > Instalación manual**.

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

   - Sitio de soporte de NetApp (necesario si aún no tiene acceso a la consola) "Sitio de soporte de NetApp" ,
3. Asignar permisos para ejecutar el script.

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

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

4. Si realiza la instalación en un entorno de nube gubernamental, desactive las comprobaciones de configuración."Aprenda cómo deshabilitar las comprobaciones de configuración para instalaciones manuales."
5. Ejecute el script de instalación.

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

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

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

+

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

firmado por una CA:

+

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

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

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

+ Ten en cuenta lo siguiente:

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

+ Por ejemplo:

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

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

   a. SSH a la máquina virtual del agente de consola.

   b. Abra el archivo podman */usr/share/containers/containers.conf* y modifique el puerto elegido para el servicio DNS de Aardvark. Por ejemplo, cámbielo a 54.

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

      Por ejemplo:

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

a. Reinicie la máquina virtual del agente de consola.

Resultado

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

¿Que sigue?

Configurar la NetApp Console.

Paso 2: Configurar la NetApp Console

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

Antes de empezar

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

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

Pasos

1. Abra un navegador web desde un host que tenga una conexión a la instancia del agente de consola e ingrese la siguiente URL del agente de consola que instaló.
2. Regístrese o inicie sesión en la NetApp Console.
3. Después de iniciar sesión, configure la consola:

    a. Introduzca un nombre para el agente de consola.

    b. Introduzca un nombre para una nueva organización de la consola.

    c. Seleccione **¿Está ejecutando en un entorno seguro?**

    d. Seleccione **Habilitar modo restringido en esta cuenta**.

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

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

    a. Seleccione **Comencemos**.

Resultado

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

¿Que sigue?

Proporcione a la consola los permisos que configuró previamente.

Paso 3: Proporcionar permisos al agente de la consola

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

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

"Aprenda a preparar los permisos en la nube" .

Rol de AWS IAM

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

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

Pasos

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

Clave de acceso de AWS

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

Pasos

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

Rol de Azure

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

Pasos

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

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

   "Documentación de Microsoft Azure: Comprender el alcance de Azure RBAC"

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

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

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

entidad de servicio de Azure

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

Pasos

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

Resultado

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

Cuenta de servicio de Google Cloud

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

Pasos

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

    "Documentación de Google Cloud: Cómo cambiar la cuenta de servicio y los ámbitos de acceso de una instancia"

2. Si desea administrar recursos en otros proyectos, otorgue acceso agregando la cuenta de servicio con el rol de agente de consola a ese proyecto. Necesitarás repetir este paso para cada proyecto.

Suscribirse a NetApp Intelligent Services (modo restringido)

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

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

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

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

Antes de empezar

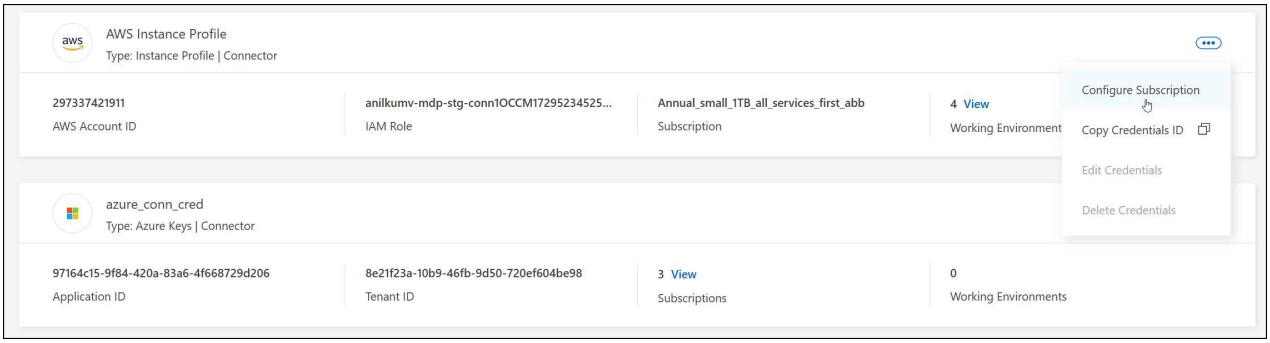
Debe haber implementado previamente un agente de consola para poder suscribirse a los servicios de datos. Debe asociar una suscripción de mercado a las credenciales de la nube conectadas a un agente de consola.

AWS

Pasos

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

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



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

   a. Seleccione **Ver opciones de compra**.

   b. Seleccione **Suscribirse**.

   c. Seleccione **Configurar su cuenta**.

      Serás redirigido a la NetApp Console.

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

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

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

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

   ◦ Seleccione **Guardar**.

Azur

Pasos

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

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

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

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

      Serás redirigido a la NetApp Console.

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

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

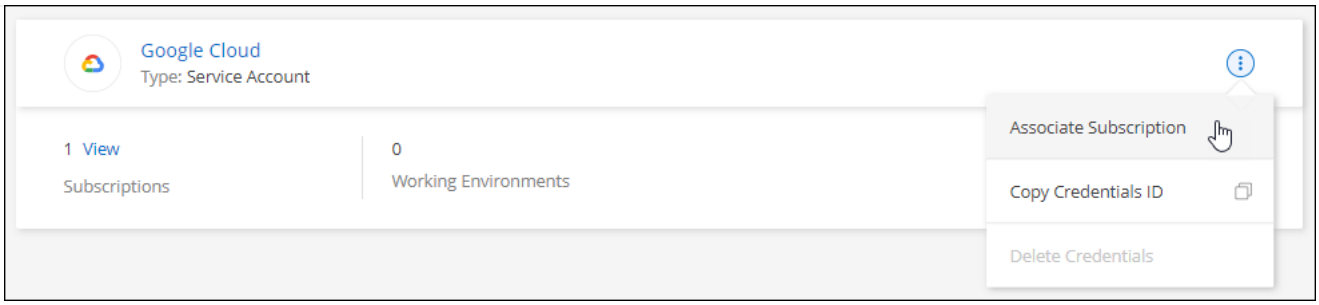
   Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.

      - Seleccione **Guardar**.

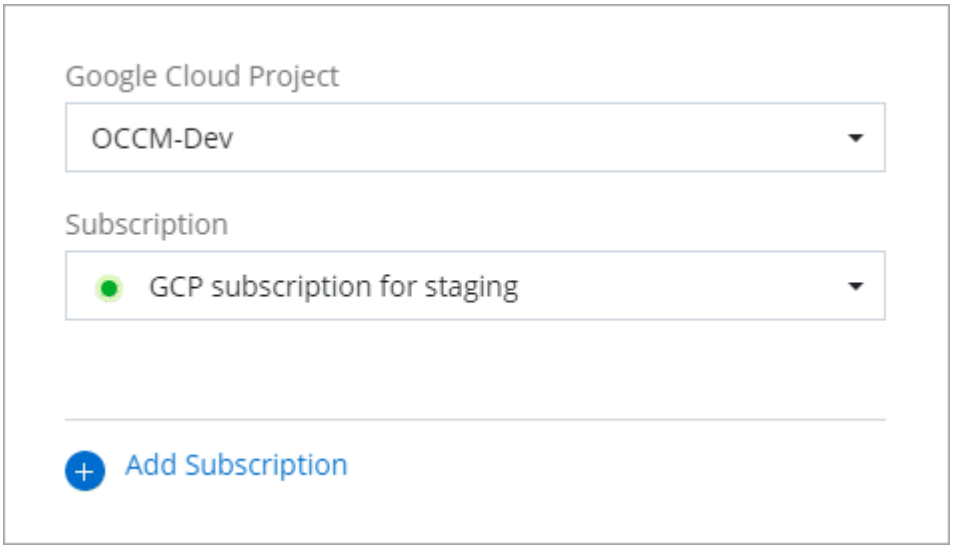
Google Cloud

Pasos

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



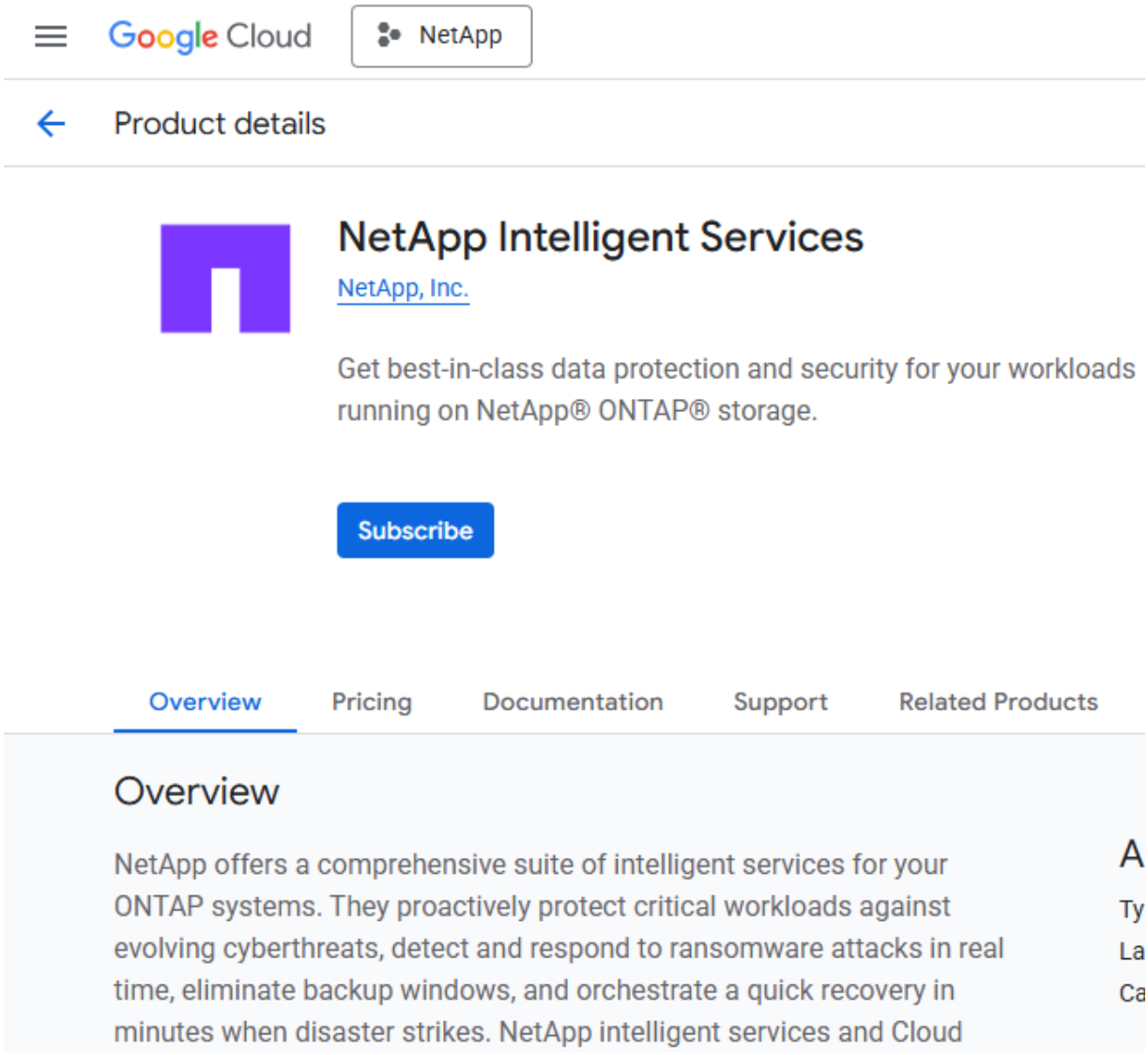
1. Para configurar una suscripción existente con las credenciales seleccionadas, seleccione un proyecto y una suscripción de Google Cloud de la lista desplegable y luego seleccione **Configurar**.



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

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

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

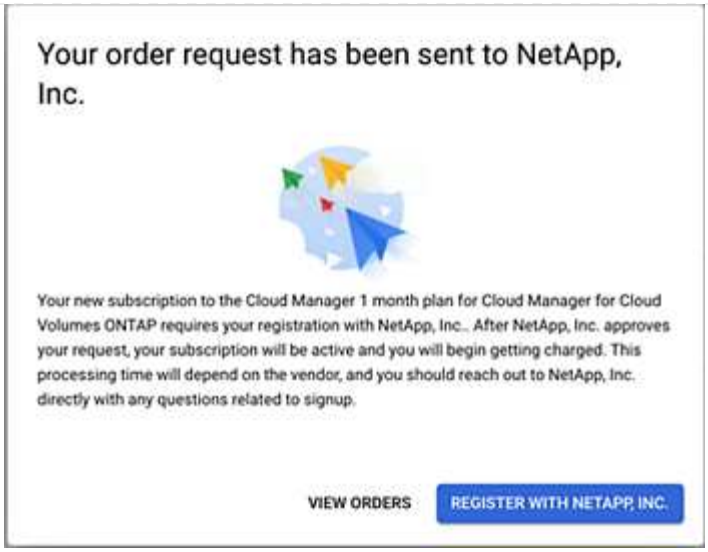


b. Seleccione **Suscribirse**.
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.
d. Seleccione **Suscribirse**.

   Este paso envía su solicitud de transferencia a NetApp.

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

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



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

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

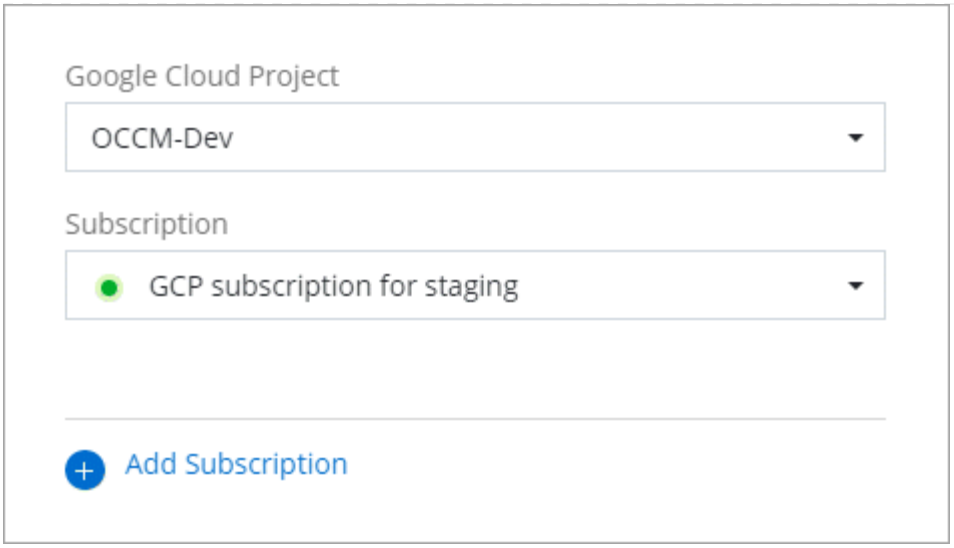
- Seleccione la organización de la consola con la que desea asociar esta suscripción.
- En el campo **Reemplazar suscripción existente**, elija si desea reemplazar automáticamente la suscripción existente de una organización con esta nueva suscripción.

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

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

- Seleccione **Guardar**.

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



Información relacionada

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

Qué puedes hacer a continuación (modo restringido)

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

Para obtener ayuda, consulte la documentación de estos servicios:

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

Información relacionada

"Modos de implementación de la NetApp Console"

Empieza con el modo privado

Flujo de trabajo de introducción (modo privado de BlueXP)

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

"Documentación en PDF para el modo privado de BlueXP"

Funciones y servicios de datos compatibles con el modo privado

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

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

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

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

Utilice la NetApp Console

Inicie sesión en la NetApp Console

La forma de iniciar sesión en la NetApp Console depende del modo de implementación que esté utilizando.

Su sesión se cerrará automáticamente después de 24 horas o si cierra su navegador.

"Obtenga más información sobre los modos de implementación de la consola" .

Modo estándar

Después de registrarse en la NetApp Console, puede iniciar sesión desde la consola basada en web para comenzar a administrar sus datos y su infraestructura de almacenamiento.

Acerca de esta tarea

Puede iniciar sesión en la NetApp Console mediante una de las siguientes opciones:

- Sus credenciales existentes del sitio de soporte de NetApp (NSS)
- Una cuenta de NetApp Console que utiliza su dirección de correo electrónico y una contraseña
- Una conexión federada

  Puede utilizar el inicio de sesión único para iniciar sesión con las credenciales de su directorio corporativo (identidad federada). "Aprenda a configurar la federación de identidades" .

Pasos

1. Abra un navegador web y vaya a "NetApp Console"
2. En la página **Iniciar sesión**, ingrese la dirección de correo electrónico asociada con su inicio de sesión.
3. Dependiendo del método de autenticación asociado con su inicio de sesión, se le solicitará que ingrese sus credenciales:
   - Credenciales de la nube de NetApp : Ingrese su contraseña
   - Usuario federado: Ingrese sus credenciales de identidad federada
   - Cuenta del sitio de soporte de NetApp : Ingrese sus credenciales del sitio de soporte de NetApp

Resultado

Ya ha iniciado sesión y puede comenzar a usar para administrar su infraestructura híbrida de múltiples nubes.

Modo restringido

Cuando utiliza la consola en modo restringido, debe iniciar sesión en la consola desde la interfaz de usuario que se ejecuta localmente en el agente.

Acerca de esta tarea

La consola admite el inicio de sesión con una de las siguientes opciones cuando está en modo restringido:

- Un inicio de sesión en la NetApp Console usando su dirección de correo electrónico y una contraseña
- Una conexión federada

  Puede utilizar el inicio de sesión único para iniciar sesión con las credenciales de su directorio corporativo (identidad federada). "Aprenda a utilizar la federación de identidades" .

Pasos

1. Abra un navegador web e ingrese la dirección IP donde está instalado el agente.
2. Introduzca su nombre de usuario y contraseña para iniciar sesión.

Trabajar con múltiples agentes de consola

Si utiliza varios agentes de consola, puede cambiar entre ellos directamente desde la consola para ver los sistemas asociados.

Cambiar entre agentes de la consola

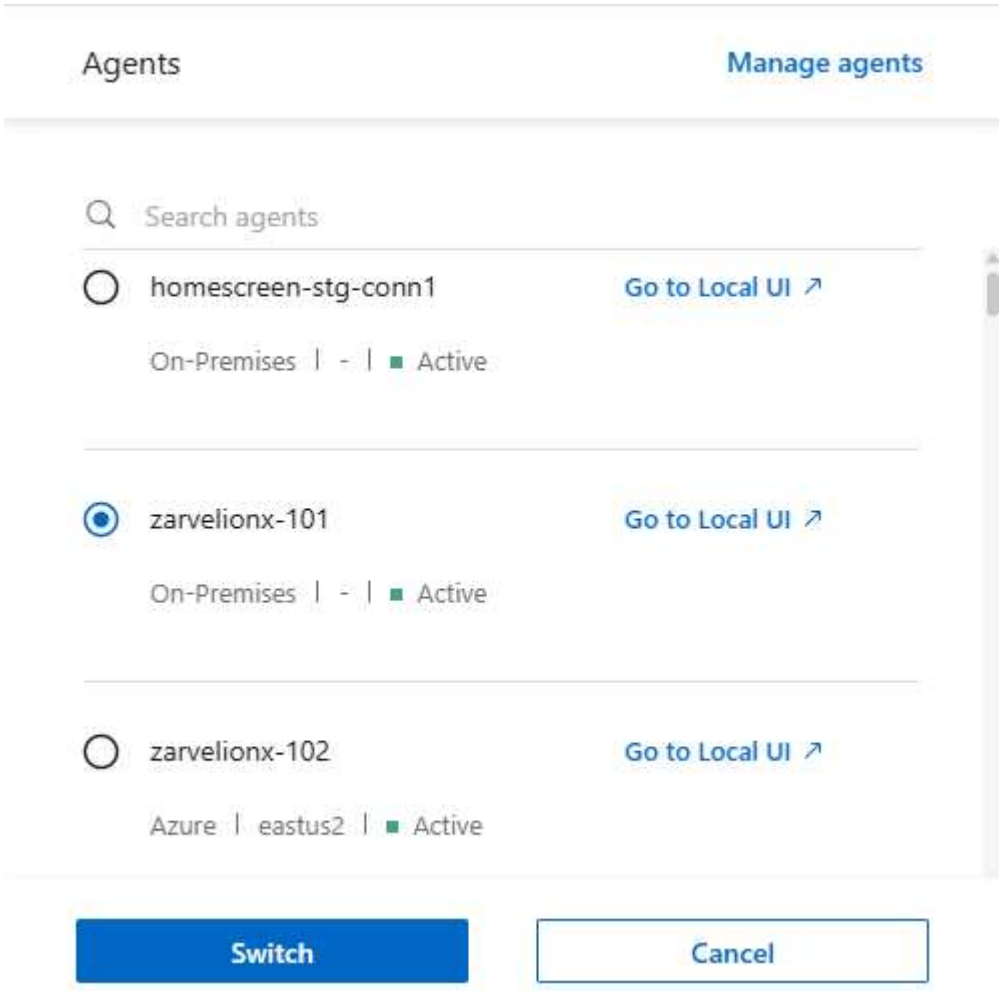
Si tiene varios agentes de consola, puede alternar entre ellos para ver los sistemas que están asociados con un agente específico.

Por ejemplo, en un entorno de múltiples nubes, es posible que tenga un agente en AWS y otro en Google Cloud. Cambie entre estos agentes para administrar los sistemas Cloud Volumes ONTAP en los respectivos entornos de nube.

Esta opción no está disponible al visualizar la NetApp Console desde la interfaz de usuario local del agente

Paso

1. Seleccione el icono de Agentes de la consola ( ) en la parte superior derecha para ver la lista de agentes disponibles.



Resultado

La consola se actualiza y muestra los sistemas asociados con el agente seleccionado.

Ver métricas en la página de inicio de la NetApp Console

Monitorear el estado de su parque de almacenamiento le permite estar al tanto de los problemas con la protección del almacenamiento y tomar medidas para resolverlos. Al utilizar la página de inicio de la NetApp Console , vea el estado de sus copias de seguridad y restauraciones de NetApp Backup and Recovery y la cantidad de cargas de trabajo que están en riesgo de sufrir un ataque de ransomware o que están protegidas según lo indicado por NetApp Ransomware Resilience. Puede revisar la capacidad de almacenamiento de clústeres individuales y Cloud Volumes ONTAP, las alertas de ONTAP , la capacidad de rendimiento de almacenamiento por clúster o sistema Cloud Volumes ONTAP , los diferentes tipos de licencias que tiene y más.

Todos los paneles de la página de inicio muestran datos a nivel de organización. Los paneles Capacidad de almacenamiento y Rendimiento de almacenamiento muestran los sistemas asociados con proyectos a los que el usuario puede acceder según los permisos de IAM.

El sistema actualiza los datos de la página de inicio cada cinco minutos. El almacenamiento en caché puede provocar que los datos de esta página difieran de los valores reales durante hasta 15 minutos.

Para obtener métricas precisas en la página de inicio se requieren agentes de consola configurados y de tamaño adecuado.

Roles requeridos de la NetApp Console

Cada panel de la página de inicio requiere diferentes roles de usuario:

- **Panel de capacidad de almacenamiento**: Capacidad para ver la página de sistemas de la NetApp Console
- *Panel de alertas de ONTAP *: Administrador de carpeta o proyecto, Analista de soporte de operaciones, Administrador de la organización, Visor de la organización, Superadministrador, Supervisor
- **Panel de capacidad de rendimiento de almacenamiento**: Capacidad para ver la página de sistemas de la NetApp Console
- * Panel de Licenses and subscriptions *: Administrador de carpeta o proyecto, Administrador de organización, Visor de organización, Superadministrador, Supervisor
- **Panel de resiliencia ante ransomware**: Administrador de carpeta o proyecto, Administrador de organización, Administrador de resiliencia ante ransomware, Visor de resiliencia ante ransomware, Superadministrador, Supervisor
- **Panel de copia de seguridad y recuperación**: Administrador de copias de seguridad de copia de seguridad y recuperación, Superadministrador de copia de seguridad y recuperación, Visor de copias de seguridad de copia de seguridad y recuperación, Administrador de clones de copia de seguridad y recuperación, Administrador de carpetas o proyectos, Administrador de la organización, Administrador de restauración de copia de seguridad y recuperación, Superadministrador, Supervisor

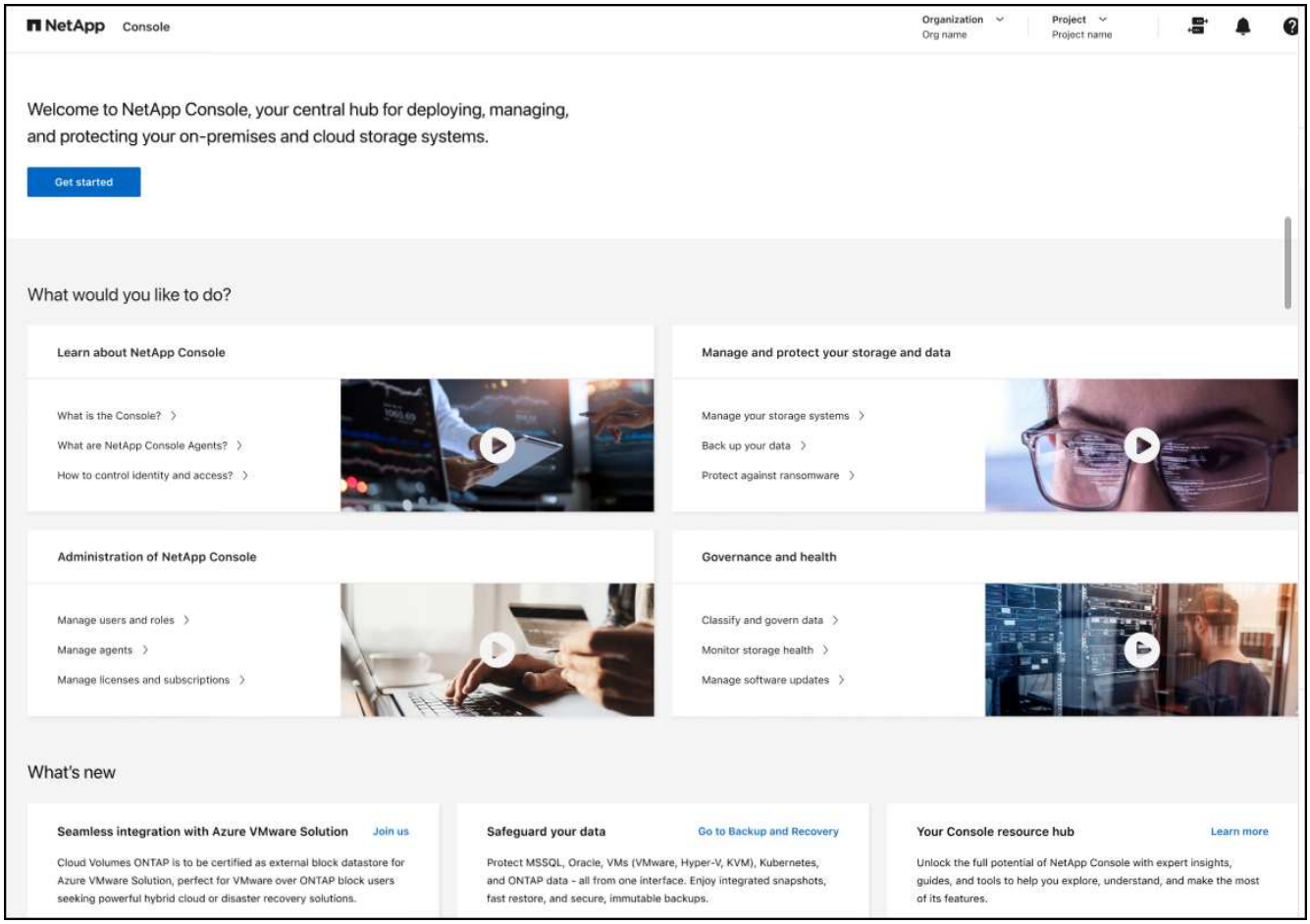
Si no tiene permisos para acceder a un panel, éste mostrará un mensaje indicando que no tiene permisos para usarlo.

"Obtenga información sobre los roles de acceso a la NetApp Console ." .

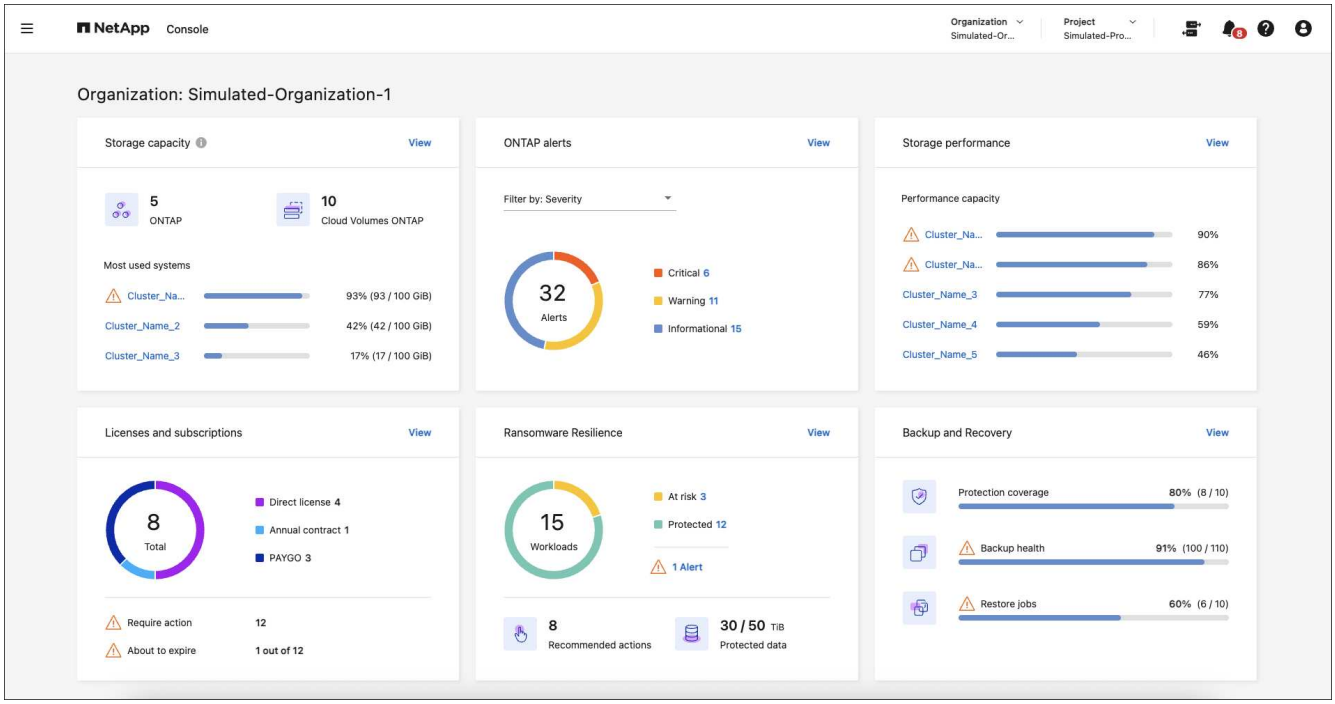
Pasos

1. Desde el menú de la NetApp Console , seleccione **Inicio**.

   Si tiene el rol de administrador de la organización y no hay ningún agente ni sistema de almacenamiento configurados, la página de inicio muestra información de inicio.



   Si ya configuró la NetApp Console, al menos un agente de consola está habilitado y se agregó al menos un clúster o sistema Cloud Volumes ONTAP a ese agente, la página de inicio muestra métricas sobre su entorno de almacenamiento.



Habilitar que las métricas aparezcan en la página de inicio

Podrás ver las métricas en la página de inicio cuando se cumplan las siguientes condiciones:

- Ha iniciado sesión en una instancia SaaS de la NetApp Console.
- Pertenece a una organización con recursos de almacenamiento existentes (agente y clúster o sistema Cloud Volumes ONTAP).
- Al menos un agente de consola está habilitado.
- Se ha agregado al menos un clúster o sistema Cloud Volumes ONTAP a ese agente.

Para permitir que las métricas aparezcan en la página de inicio, complete las siguientes tareas:

- Habilite al menos un agente de consola.
- Agregue al menos un clúster o un Cloud Volumes ONTAP usando ese agente.

Ver la capacidad de almacenamiento general

El panel Capacidad de almacenamiento proporciona la siguiente información sobre los clústeres de ONTAP y los sistemas Cloud Volumes ONTAP :

- Número de sistemas ONTAP descubiertos en la consola
- Número de sistemas Cloud Volumes ONTAP detectados en la consola
- Uso de capacidad por clúster

El orden de los clústeres o sistemas Cloud Volumes ONTAP se basa en la cantidad de capacidad utilizada. El clúster o sistema con mayor capacidad aparece primero para una fácil identificación.

Los indicadores de advertencia muestran grupos con una capacidad del 80% y los datos se actualizan cada cinco minutos.

Si tiene varios proyectos, es posible que vea datos diferentes en el panel Capacidad de almacenamiento en comparación con la página Sistemas. Esto se debe a que la página Sistemas muestra información según el nivel de proyecto, mientras que el panel Capacidad de almacenamiento muestra información a nivel de organización. Además, los datos de este panel pueden diferir de los valores reales durante un máximo de 15 minutos porque los datos se almacenan en caché durante ese período para optimizar el rendimiento.

Pasos

1. Desde el menú de la NetApp Console , revise el panel Capacidad de almacenamiento.
2. En el panel Capacidad de almacenamiento, seleccione **Ver** para ir a la página Sistemas de consola.
3. En la página Sistemas, seleccione el proyecto que contiene el clúster que desea ver.
4. En la página Sistemas, seleccione un clúster para ver más detalles sobre ese clúster.

Ver alertas de ONTAP

Vea problemas o riesgos potenciales en sus entornos ONTAP locales de NetApp . Puedes ver algunas alertas que no son de EMS y algunas alertas de EMS.

Los datos se actualizan cada 5 minutos.

Puedes ver alertas de ONTAP con estos niveles de gravedad:

- Crítico
- Advertencia
- Informativo

Puede ver las alertas de ONTAP para estas áreas de impacto:

- Capacidad
- Actuación
- Protection
- Disponibilidad
- Seguridad

El almacenamiento en caché optimiza el rendimiento, pero puede provocar que los datos de este panel difieran de los valores reales durante hasta 15 minutos.

Sistemas compatibles

- Se admite un sistema NAS o SAN ONTAP local.
- Los sistemas Cloud Volumes ONTAP no son compatibles.

Fuentes de datos compatibles

Ver alertas sobre ciertos eventos que ocurren en ONTAP. Son una combinación de EMS y alertas basadas en métricas.

Para obtener detalles sobre las alertas de ONTAP , consulte "Acerca de las alertas de ONTAP" .

Para obtener una lista de alertas que podría ver, consulte "Ver los riesgos potenciales en el almacenamiento de ONTAP" .

Pasos

1. Desde el menú de la NetApp Console , revise el panel de alertas de ONTAP .
2. Opcionalmente, filtre las alertas seleccionando el nivel de gravedad o cambie el filtro para mostrar alertas según el área de impacto.
3. En el panel de alertas de ONTAP , seleccione **Ver** para ir a la página Alertas de la consola.

Ver la capacidad de rendimiento del almacenamiento

Revise la capacidad de rendimiento de almacenamiento utilizada por clúster o sistema Cloud Volumes ONTAP para determinar cómo la capacidad de rendimiento, la latencia y las IOPS afectan sus cargas de trabajo. Por ejemplo, es posible que descubra que necesita cambiar las cargas de trabajo para minimizar la latencia y maximizar las IOPS y el rendimiento de sus cargas de trabajo críticas.

El sistema organiza los clústeres y sistemas según su capacidad de rendimiento, enumerando primero la capacidad más alta para una fácil identificación.

El almacenamiento en caché optimiza el rendimiento, pero puede provocar que los datos de este panel difieran de los valores reales durante hasta 15 minutos.

Pasos

1. Desde el menú de la NetApp Console , revise el panel Rendimiento de almacenamiento.
2. En el panel Rendimiento de almacenamiento, seleccione **Ver** para ir a una página Rendimiento que enumera todos los clústeres y los datos de los sistemas Cloud Volumes ONTAP sobre capacidad de rendimiento, IOPS y latencia.
3. Seleccione un clúster para ver sus detalles en el Administrador del sistema.

Ver las licencias y suscripciones que tienes

Revise la siguiente información en el panel Licenses and subscriptions :

- El número total de licencias y suscripciones que tiene.
- El número de cada tipo de licencia y suscripción que tienes (licencia directa, contrato anual o PAYGO).
- La cantidad de licencias y suscripciones que están activas, requieren acción o están próximas a vencer.
- El sistema muestra indicadores junto a los tipos de licencia que requieren acción o están próximos a vencer.

Los datos se actualizan cada 5 minutos.

El almacenamiento en caché optimiza el rendimiento, pero puede provocar que los datos de este panel difieran de los valores reales durante hasta 15 minutos.

Pasos

1. Desde el menú de la NetApp Console , revise el panel Licenses and subscriptions .
2. En el panel Licenses and subscriptions , seleccione **Ver** para ir a la página Licenses and subscriptions de la consola.

Ver el estado de resiliencia frente al ransomware

Descubra si las cargas de trabajo están en riesgo de ataques de ransomware o están protegidas con el servicio de datos NetApp Ransomware Resilience . Puede revisar la cantidad total de datos que están protegidos, ver la cantidad de acciones recomendadas y ver la cantidad de alertas relacionadas con la protección contra ransomware.

Los datos se actualizan cada 5 minutos y coinciden con los datos que se muestran en el Panel de NetApp Ransomware Resilience .

"Obtenga más información sobre la NetApp Ransomware Resilience" .

Pasos

1. Desde el menú de la NetApp Console , revise el panel Resiliencia ante ransomware.
2. Realice una de las siguientes acciones en el panel Resiliencia ante ransomware:
   - Seleccione **Ver** para ir al Panel de NetApp Ransomware Resilience . Para más detalles, consulte "Supervise el estado de la carga de trabajo mediante el panel de NetApp Ransomware Resilience" .
   - Revise las “Acciones recomendadas” en el Panel de NetApp Ransomware Resilience . Para más detalles, consulte "Revise las recomendaciones de protección en el Panel de NetApp Ransomware Resilience" .
   - Seleccione el enlace de alertas para revisar las alertas en la página de alertas de NetApp Ransomware Resilience . Para más detalles, consulte "Gestione las alertas de ransomware detectadas con NetApp Ransomware Resilience" .

Ver el estado de la copia de seguridad y recuperación

Revise el estado general de sus copias de seguridad y restauraciones desde NetApp Backup and Recovery. Puede ver la cantidad de recursos protegidos y no protegidos. También puede ver el porcentaje de operaciones de copias de seguridad y restauración para la protección de sus cargas de trabajo. Un porcentaje más alto indica una mejor protección de datos.

Los datos se actualizan cada 5 minutos.

El almacenamiento en caché optimiza el rendimiento, pero puede provocar que los datos de este panel difieran de los valores reales durante hasta 15 minutos.

Pasos

1. Desde el menú de la NetApp Console , revise el panel Copia de seguridad y recuperación.
2. Seleccione **Ver** para ir al Panel de control de NetApp Backup and Recovery . Para más detalles, consulte "Documentación de NetApp Backup and Recovery" .

Administrar la configuración de usuario de la NetApp Console

Puede modificar su perfil de consola, lo que incluye cambiar su contraseña, habilitar la autenticación multifactor (MFA) y ver quién es su administrador de consola.

Dentro de la Consola, cada usuario tiene un perfil que contiene información sobre el usuario y su configuración. Puede ver y editar la configuración de su perfil.

Cambiar tu nombre para mostrar

Puedes cambiar el nombre para mostrar de tu consola, que te identifica ante otros usuarios. No puedes cambiar tu nombre de usuario ni dirección de correo electrónico.

Pasos

1. Seleccione el ícono de perfil en la esquina superior derecha de la Consola para ver el panel de configuración de Usuario.
2. Seleccione el ícono **Editar** junto a su nombre.
3. Ingrese su nuevo nombre para mostrar en el campo **Nombre**.

Mejora tu rol en modo de solo lectura

En algunos casos, el administrador de su organización puede poner su organización en modo de solo lectura. Si tiene un rol de administrador, debe elevar los permisos para realizar cambios. Esto garantiza que los cambios sean intencionales y autorizados.

Después de elevar su rol, podrá realizar cambios en la Consola hasta que expire su sesión actual.

Cuando haya terminado, cierre la sesión de la consola o mueva el control deslizante hacia atrás para regresar al modo de solo lectura. El sistema elimina sus permisos elevados cuando su sesión expira.

Pasos

1. Seleccione el ícono de perfil en la esquina superior derecha de la Consola para ver el panel de configuración de Usuario.
2. Para el estado de **Modo de solo lectura**, mueva el control deslizante a la posición **Elevado** y confirme los cambios.

Configurar la autenticación multifactor

Configure la autenticación multifactor (MFA) para mejorar la seguridad al requerir un segundo método de verificación.

Los usuarios que utilizan el inicio de sesión único con un proveedor de identidad externo o el sitio de soporte de NetApp no pueden habilitar MFA. Si alguna de estas situaciones es cierta para usted, no verá la opción para habilitar MFA en la configuración de su perfil.

No habilite MFA si su cuenta de usuario se utiliza para acceder a la API. La autenticación multifactor detiene el acceso a la API cuando está habilitada para una cuenta de usuario. Utilice cuentas de servicio para todo el acceso a la API.

Antes de empezar

- Debes haber descargado ya una aplicación de autenticación, como Google Authenticator o Microsoft Authenticator, en tu dispositivo.
- Necesitará su contraseña para configurar MFA.

Si no tiene acceso a su aplicación de autenticación o pierde su código de recuperación, comuníquese con el administrador de su consola para obtener ayuda.

Pasos

1. Seleccione el ícono de perfil en la esquina superior derecha de la Consola para ver el panel de configuración de Usuario.
2. Seleccione **Configurar** junto al encabezado **Autenticación multifactor**.
3. Siga las instrucciones para configurar MFA para su cuenta.
4. Cuando termine, se le pedirá que guarde su código de recuperación. Elija copiar el código o descargar un archivo de texto que contenga el código. Guarde este código en un lugar seguro. Necesitará el código de recuperación si pierde el acceso a su aplicación de autenticación.

   Después de configurar MFA, la consola le solicitará que ingrese un código de un solo uso de su aplicación de autenticación cada vez que inicie sesión.

Regenera tu código de recuperación de MFA

Solo puedes usar los códigos de recuperación una vez. Si usas o pierdes el tuyo, crea uno nuevo.

Pasos

1. Seleccione el ícono de perfil en la esquina superior derecha de la Consola para ver el panel de configuración de Usuario.
2. Seleccionar ••• junto al encabezado **Autenticación multifactor**.
3. Seleccione **Regenerar código de recuperación**.
4. Copie el código de recuperación generado y guárdelo en una ubicación segura.

Eliminar su configuración de MFA

Cuando haya terminado, cierre la sesión de la consola o mueva el control deslizante hacia atrás para regresar al modo de solo lectura. El sistema elimina sus permisos elevados cuando su sesión expira.

Si no puede acceder a su aplicación de autenticación o código de recuperación, deberá comunicarse con el administrador de su organización para restablecer su configuración de MFA.

Pasos

1. Seleccione el ícono de perfil en la esquina superior derecha de la Consola para ver el panel de configuración de Usuario.
2. Seleccionar ••• junto al encabezado **Autenticación multifactor**.
3. Seleccione **Eliminar**.

Comuníquese con el administrador de su organización

Si necesita comunicarse con el administrador de su organización, puede enviarle un correo electrónico directamente desde la Consola. El administrador gestiona las cuentas de usuario y los permisos dentro de su organización.

Debe tener una aplicación de correo electrónico predeterminada configurada en su navegador para poder utilizar la función **Contactar a los administradores**.

Pasos

1. Seleccione el ícono de perfil en la esquina superior derecha de la Consola para ver el panel de configuración de Usuario.
2. Seleccione **Contactar a los administradores** para enviar un correo electrónico al administrador de su organización.
3. Seleccione la aplicación de correo electrónico que desea utilizar.
4. Finaliza el correo electrónico y selecciona **Enviar**.

Configurar el modo oscuro (tema oscuro)

Puedes configurar la consola para que se muestre en modo oscuro.

Pasos

1. Seleccione el ícono de perfil en la esquina superior derecha de la Consola para ver el panel de configuración de Usuario.
2. Mueva el control deslizante **Tema oscuro** para habilitarlo.

Administrar y monitorear

Asociar cuentas de soporte de NetApp

Administrar las credenciales NSS asociadas con la NetApp Console

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

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

Descripción general

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

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

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

- Registro de sistemas Cloud Volumes ONTAP de pago por uso

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

- Actualización del software Cloud Volumes ONTAP a la última versión

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

Agregar una cuenta NSS

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

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

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

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

Pasos

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

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

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

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

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

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

¿Que sigue?

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

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

Actualizar las credenciales de NSS

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

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

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

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

Pasos

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

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

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

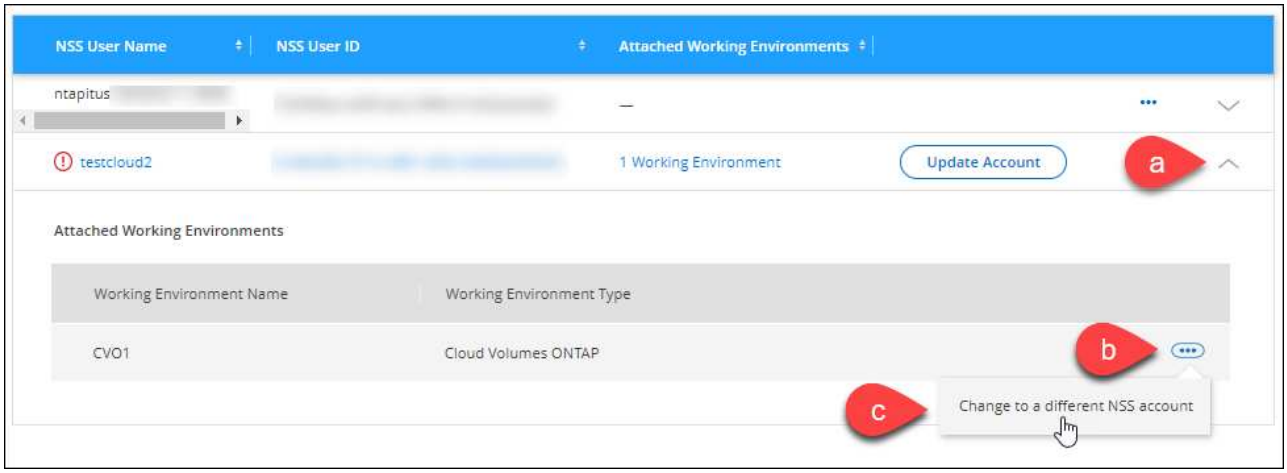
Adjuntar un sistema a una cuenta NSS diferente

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

Primero debes haber asociado la cuenta con la Consola.

Pasos

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



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

Mostrar la dirección de correo electrónico de una cuenta NSS

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

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

Pasos

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

3. Para la cuenta NSS que desea actualizar, seleccione ••• y luego seleccione **Mostrar dirección de correo electrónico**. Puede utilizar el botón Copiar para copiar la dirección de correo electrónico.

Eliminar una cuenta NSS

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

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

Pasos

1. En **Administración > Soporte**.
2. Seleccione **Administración NSS**.
3. Para la cuenta NSS que desea eliminar, seleccione ••• y luego seleccione **Eliminar**.
4. Seleccione **Eliminar** para confirmar.

Administrar las credenciales asociadas con el inicio de sesión de su NetApp Console

Según las acciones que haya realizado en la consola, es posible que haya asociado las credenciales de ONTAP y las credenciales del sitio de soporte de NetApp (NSS) con su inicio de sesión de usuario. Puede ver y administrar esas credenciales después de haberlas asociado. Por ejemplo, si cambia la contraseña de estas credenciales, deberá actualizar la contraseña en la Consola.

Credenciales de ONTAP

Los usuarios necesitan credenciales de administrador de ONTAP para descubrir clústeres de ONTAP en la consola. Sin embargo, el acceso a ONTAP System Manager depende de si está utilizando o no un agente de consola.

Sin un agente de consola

Se solicita a los usuarios que ingresen sus credenciales de ONTAP para acceder a ONTAP System Manager para el clúster. Los usuarios pueden elegir guardar estas credenciales en la consola, lo que significa que no se les solicitará que las ingresen cada vez. Las credenciales de usuario solo son visibles para el usuario respectivo y se pueden administrar desde la página Credenciales de usuario.

Con un agente de consola

De forma predeterminada, no se solicita a los usuarios que ingresen sus credenciales de ONTAP para acceder a ONTAP System Manager. Sin embargo, un administrador de la consola (con el rol de administrador de la organización) puede configurar la consola para solicitar a los usuarios que ingresen sus credenciales de ONTAP . Cuando esta configuración está habilitada, los usuarios deben ingresar sus credenciales de ONTAP cada vez.

"Más información."

Credenciales de NSS

Las credenciales de NSS asociadas con su inicio de sesión en la NetApp Console permiten el registro de soporte, la gestión de casos y el acceso a Digital Advisor.

- Cuando accede a **Soporte > Recursos** y se registra para recibir soporte, se le solicita que asocie las credenciales de NSS con su inicio de sesión.

  Esto registra su organización o cuenta para recibir soporte y activa el derecho a soporte. Solo un usuario de su organización debe asociar una cuenta del sitio de soporte de NetApp con su inicio de sesión para registrarse para recibir soporte y activar el derecho a soporte. Una vez completado esto, la página **Recursos** mostrará que su cuenta está registrada para recibir soporte.

  "Aprenda cómo registrarse para recibir soporte"

- Cuando acceda a **Administración > Soporte > Gestión de casos**, se le solicitará que ingrese sus credenciales de NSS, si aún no lo ha hecho. Esta página le permite crear y administrar los casos de soporte asociados con su cuenta NSS y con su empresa.
- Cuando accede a Digital Advisor en la consola, se le solicita que inicie sesión en Digital Advisor ingresando sus credenciales de NSS.

Tenga en cuenta lo siguiente sobre la cuenta NSS asociada con su inicio de sesión:

- La cuenta se administra a nivel de usuario, lo que significa que no puede ser vista por otros usuarios que inicien sesión.
- Solo puede haber una cuenta NSS asociada con Digital Advisor y la gestión de casos de soporte por usuario.
- Si intenta asociar una cuenta del sitio de soporte de NetApp con un sistema Cloud Volumes ONTAP , solo puede elegir entre las cuentas NSS que se agregaron a la organización de la que es miembro.

  Las credenciales de nivel de cuenta NSS son diferentes a las de la cuenta NSS asociada con su inicio de sesión. Las credenciales de nivel de cuenta de NSS le permiten implementar Cloud Volumes ONTAP con BYOL, registrar sistemas PAYGO y actualizar su software.

  "Obtenga más información sobre el uso de credenciales NSS con su organización o cuenta de NetApp Console" .

Administra tus credenciales de usuario

Administre sus credenciales de usuario actualizando el nombre de usuario y la contraseña o eliminando las credenciales.

Pasos

1. Seleccione **Administración > Credenciales**.
2. Seleccione **Credenciales de usuario**.
3. Si aún no tiene credenciales de usuario, puede seleccionar **Agregar credenciales NSS** para agregar su cuenta del sitio de soporte de NetApp .
4. Administre las credenciales existentes eligiendo las siguientes opciones en el menú Acciones:
   - **Actualizar credenciales**: Actualice el nombre de usuario y la contraseña de la cuenta.
   - **Eliminar credenciales**: elimina la cuenta NSS asociada con tu inicio de sesión en la consola.

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
Sistemas StorageGRID	Sí	No
Clúster ONTAP local (gestión y descubrimiento avanzados)	Sí (gestión y descubrimiento avanzados)	No (sólo descubrimiento básico)

	Disponible con agente	Disponible sin agente
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 .
\ 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.

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 .
\ 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 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 .
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

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 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 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.

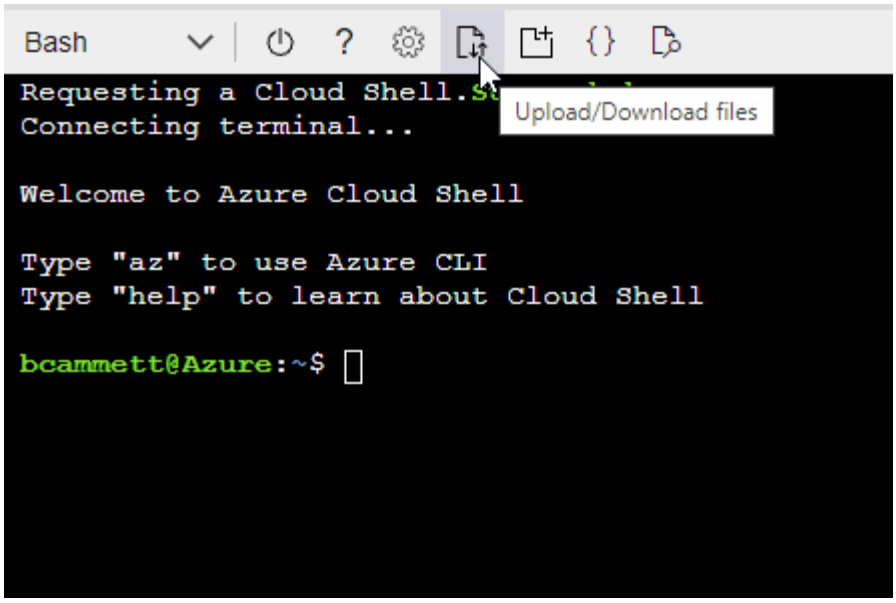
   Ejemplo

```
"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.

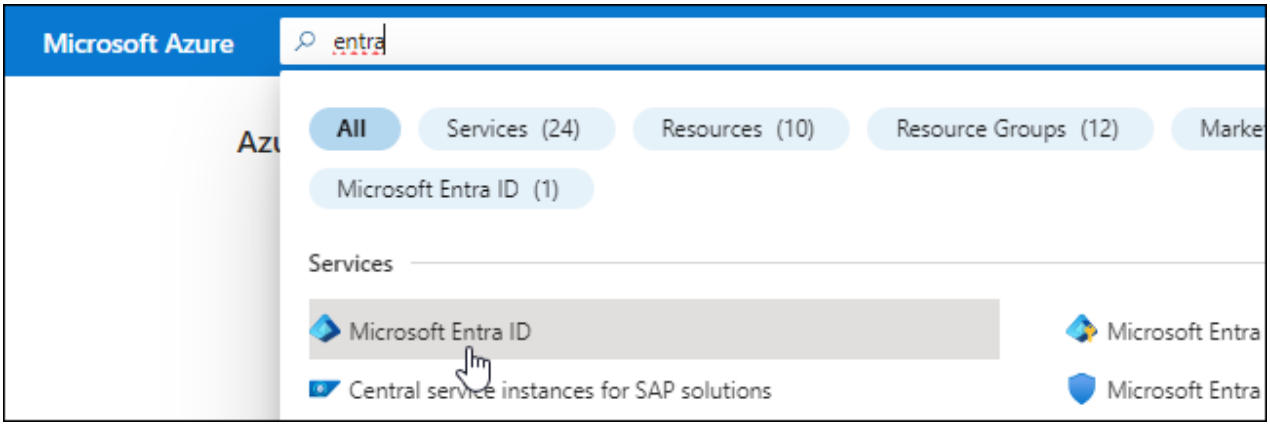
Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita la consola.

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**.

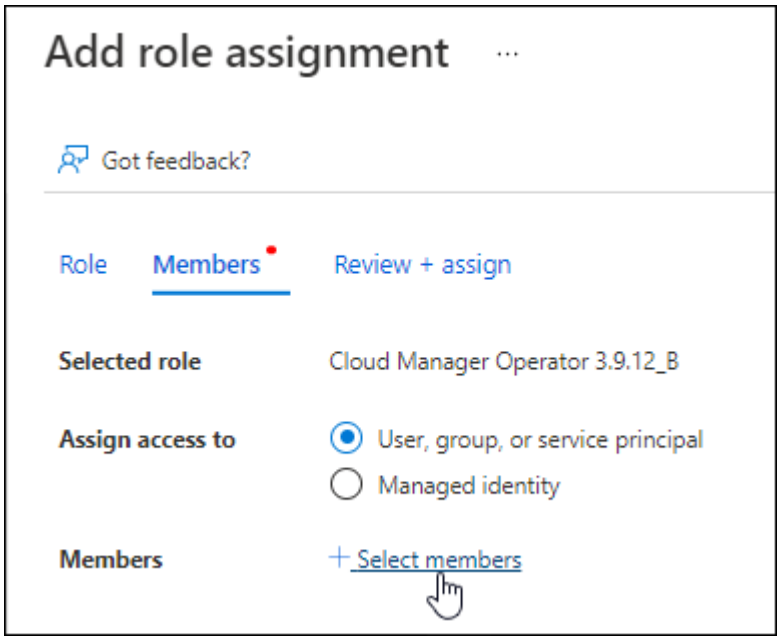
   Ha creado la aplicación AD y la entidad principal de servicio.

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:

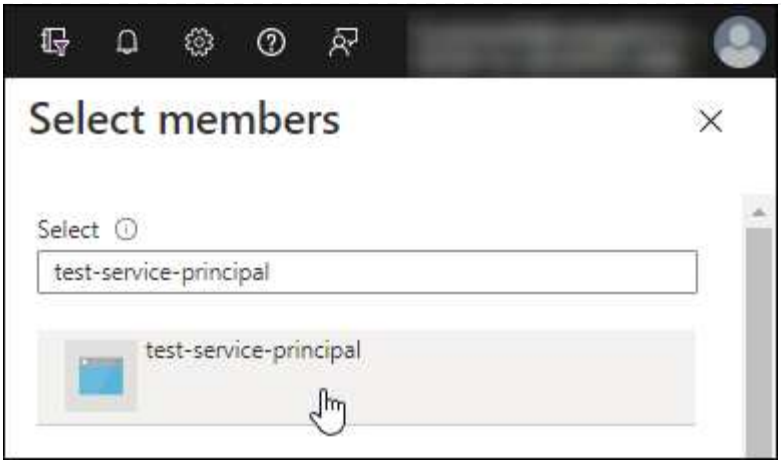
   a. Mantenga seleccionado **Usuario, grupo o entidad de servicio**.

   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**.

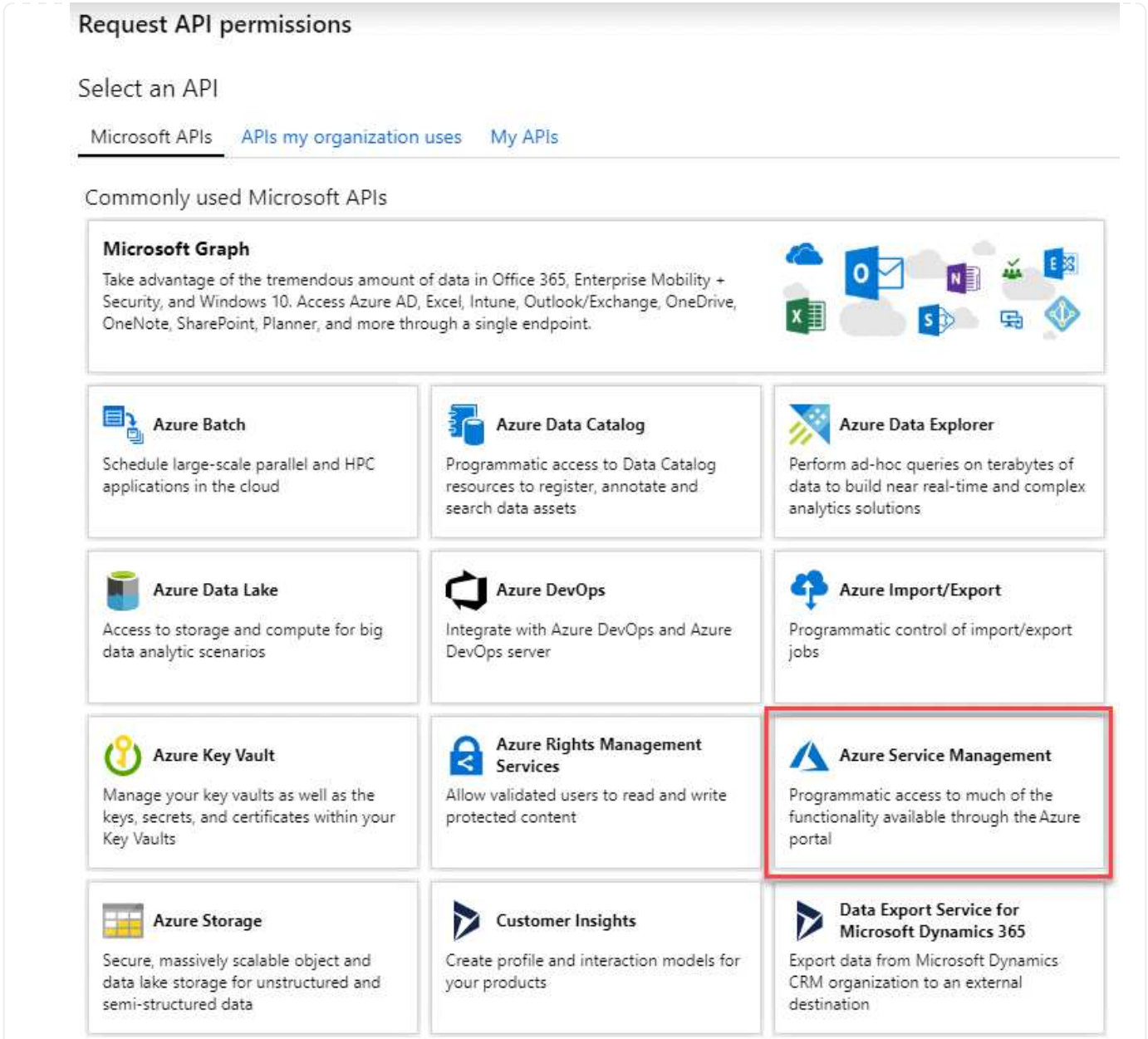
6. Haga clic en **Revisar + asignar**.

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

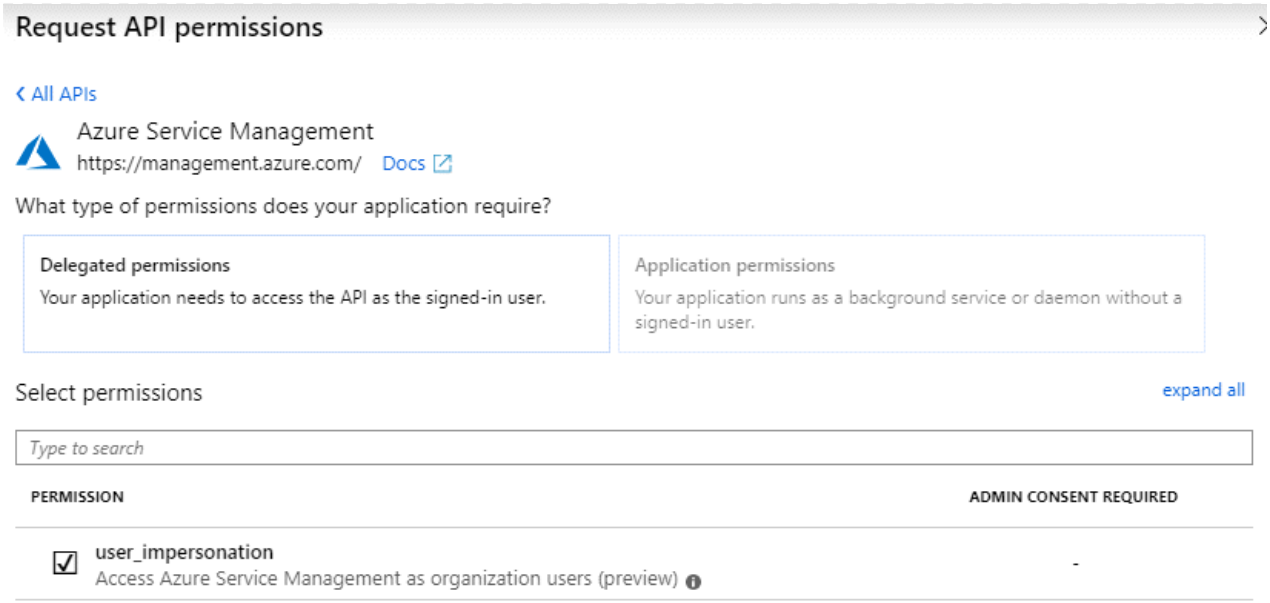
   Si desea administrar recursos en varias suscripciones de Azure, debe vincular la entidad de servicio a cada una de esas suscripciones. Por ejemplo, la consola le permite seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

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**.

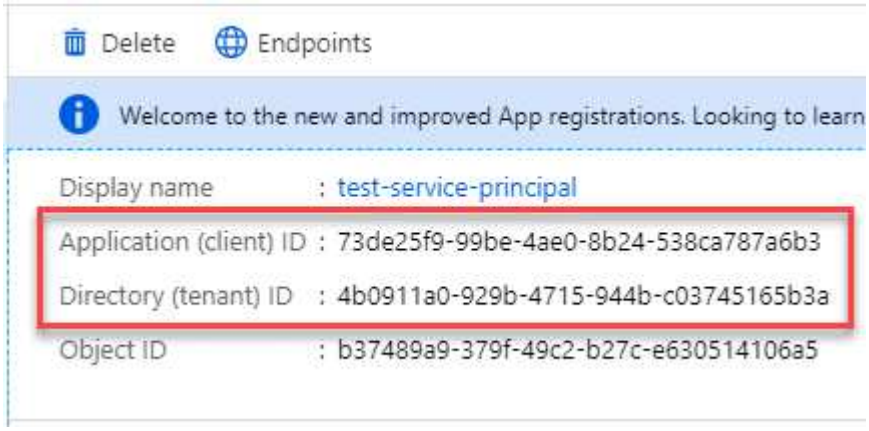


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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.

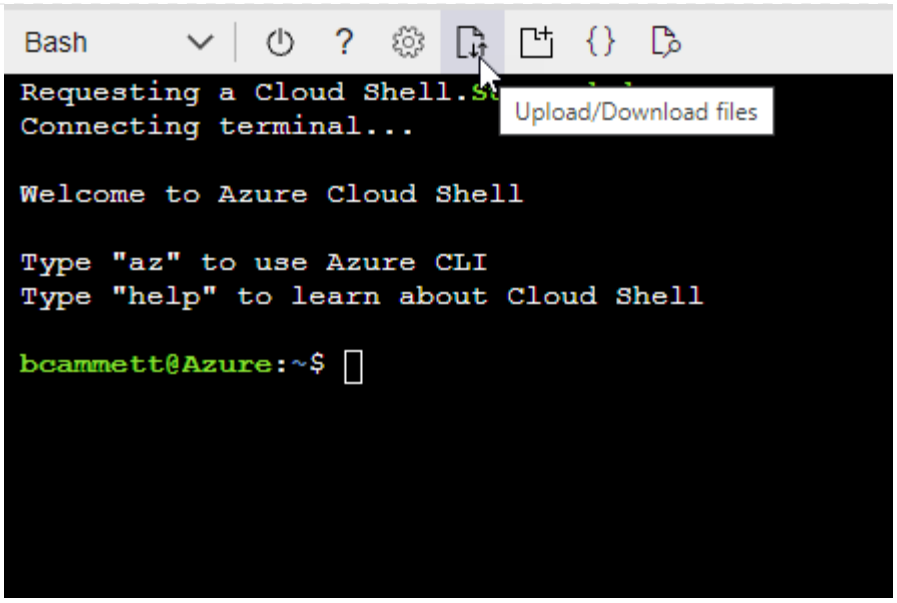
   Ejemplo

   ```
   "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

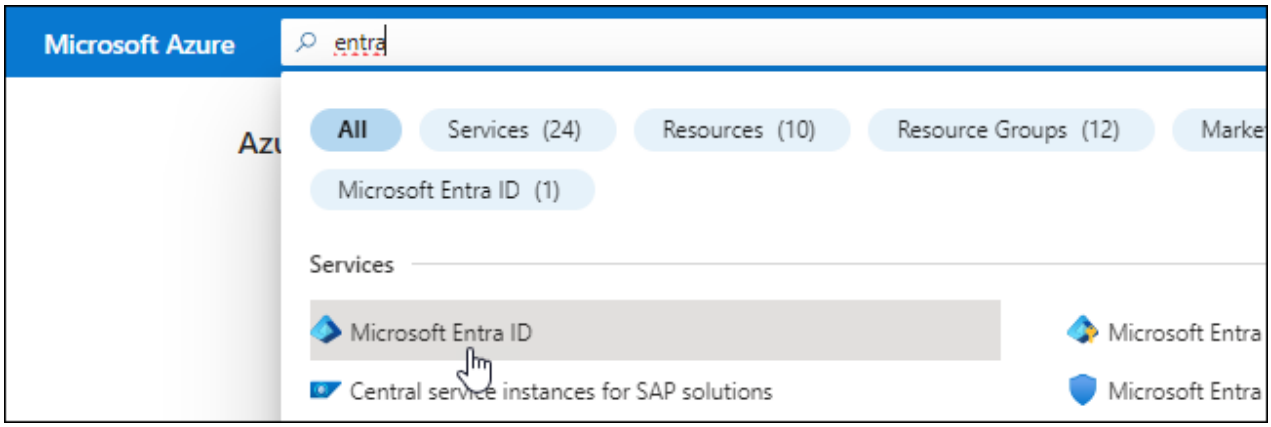
Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita la consola.

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 .

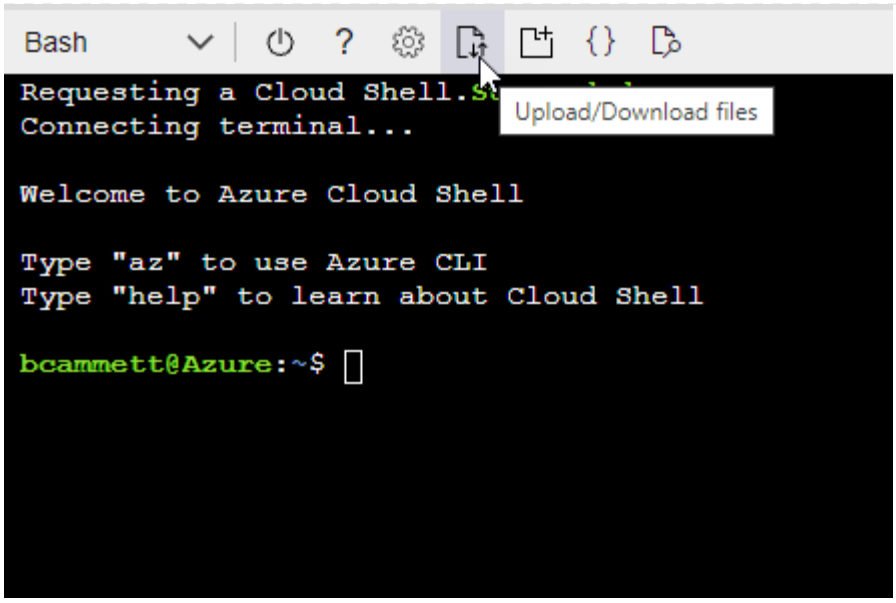
      Ejemplo

      ```
      "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**.

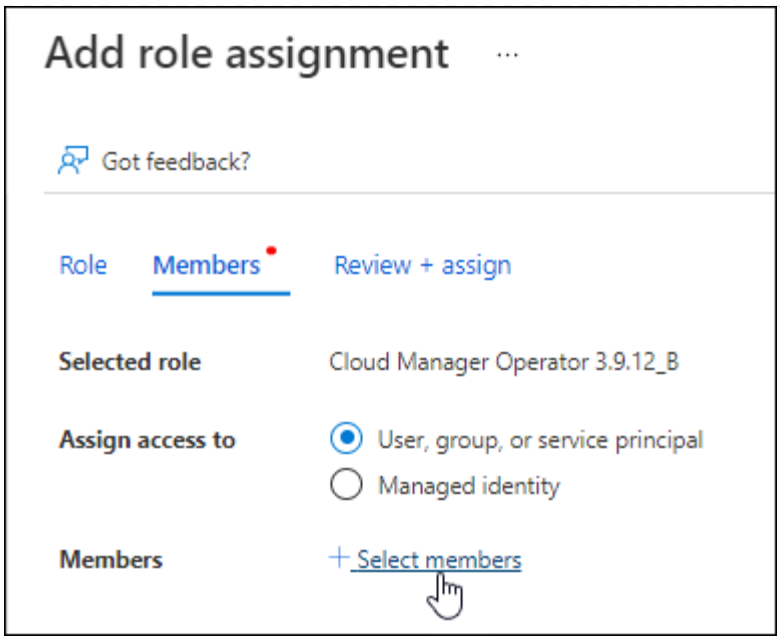
   b. Seleccione la suscripción.

   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**.

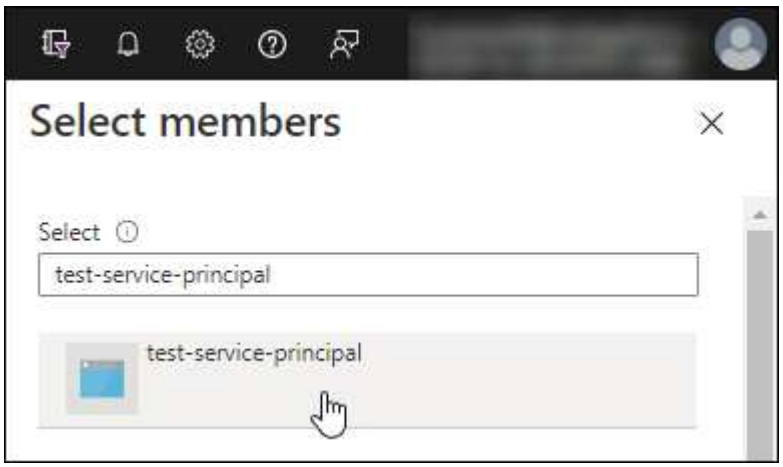
   e. En la pestaña **Miembros**, complete los siguientes pasos:

      - 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**.

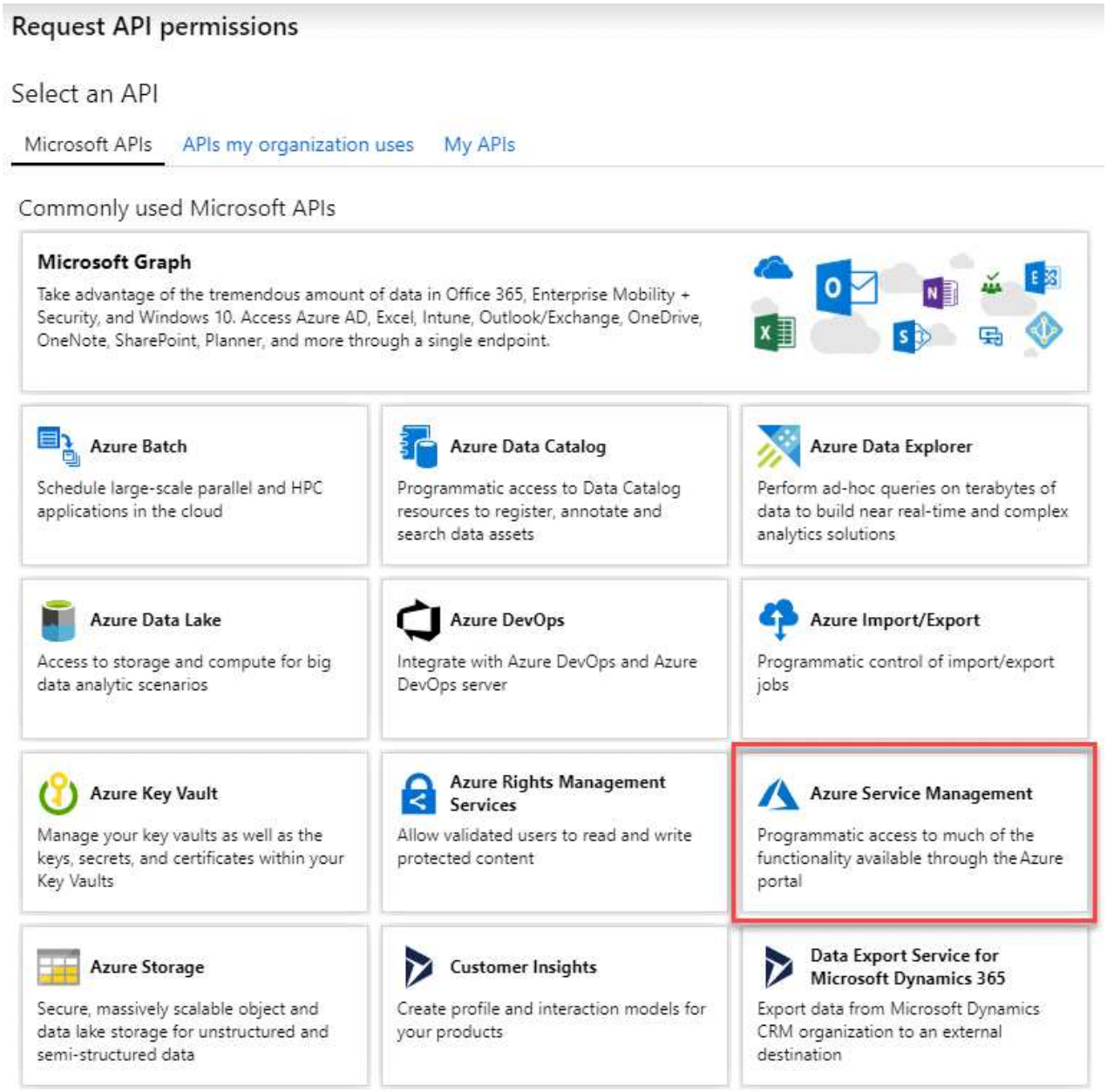
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

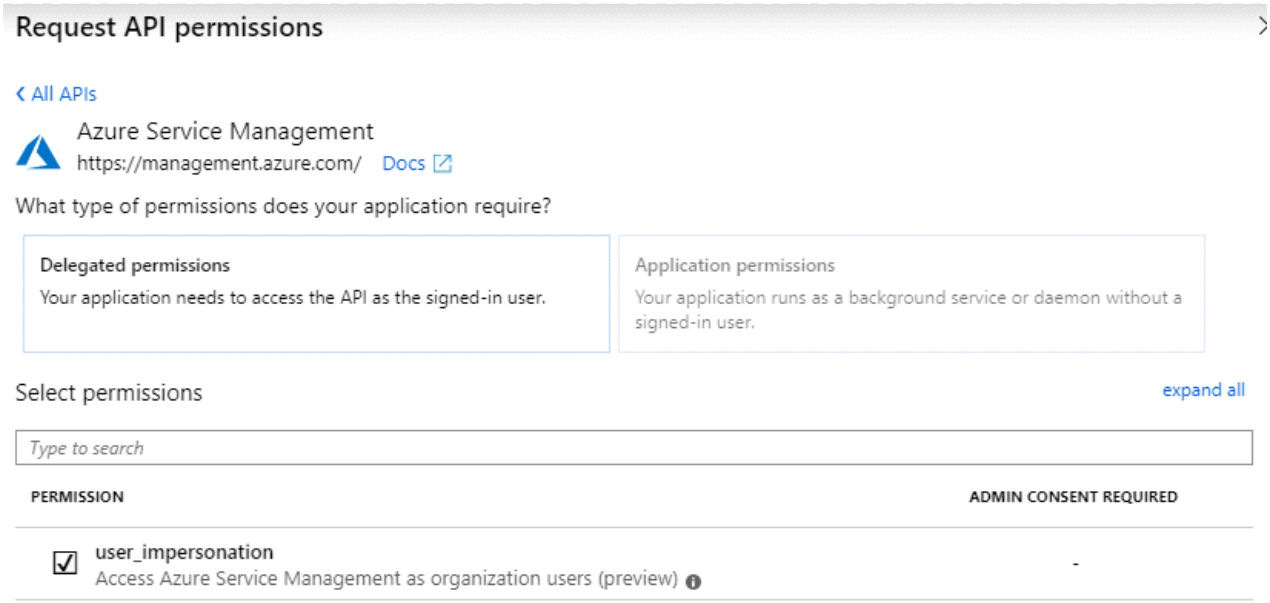
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

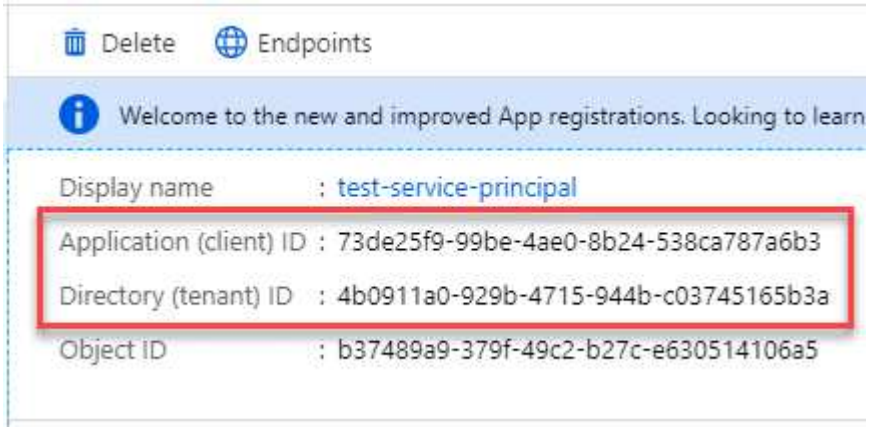


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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

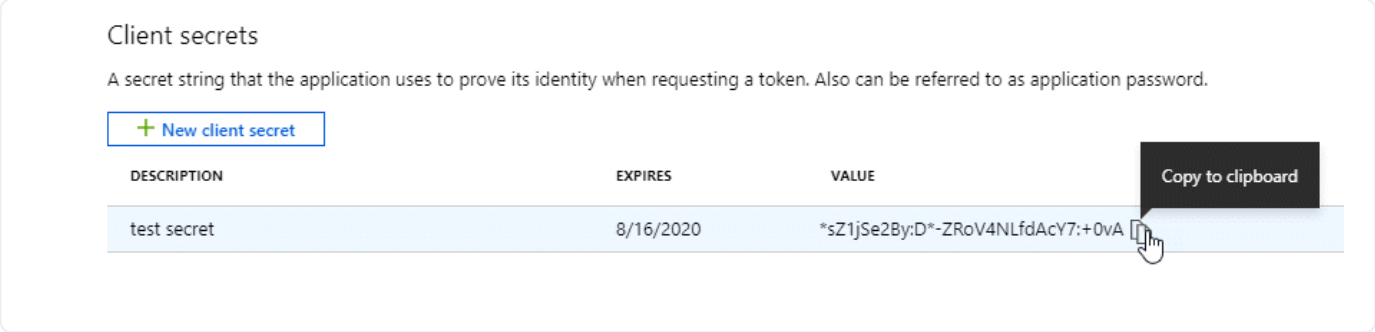
1. En el servicio **Microsoft Entra ID**, seleccione **Registros de aplicaciones** y seleccione la aplicación.
2. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)**.



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 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

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.

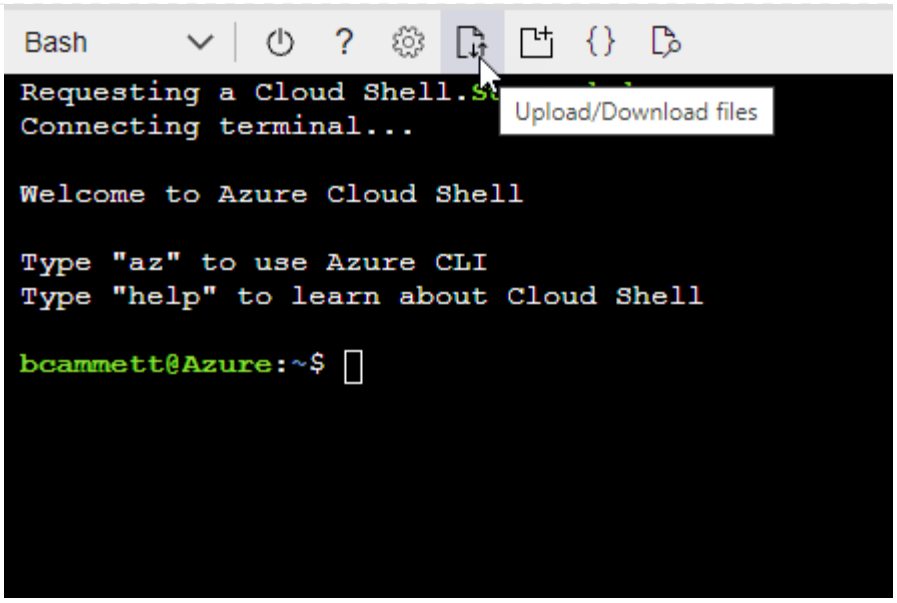
   Ejemplo

   ```
   "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

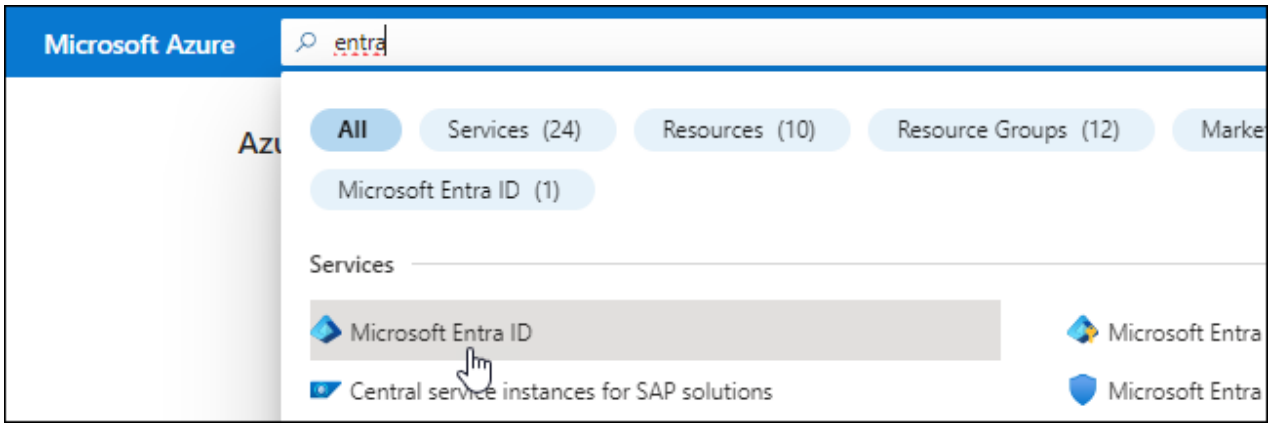
Cree y configure una entidad de servicio en Microsoft Entra ID y obtenga las credenciales de Azure que necesita el agente de consola.

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 .

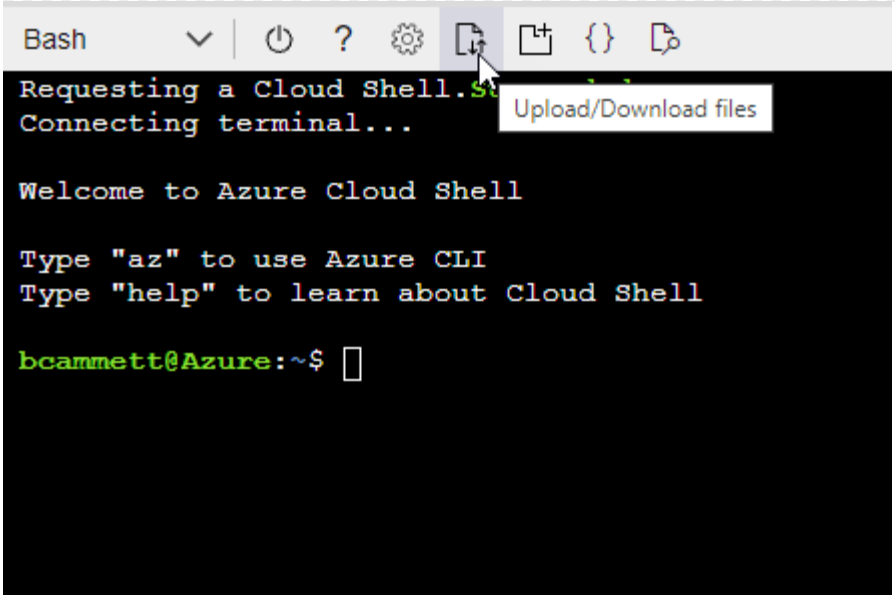
      Ejemplo

      ```
      "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**.

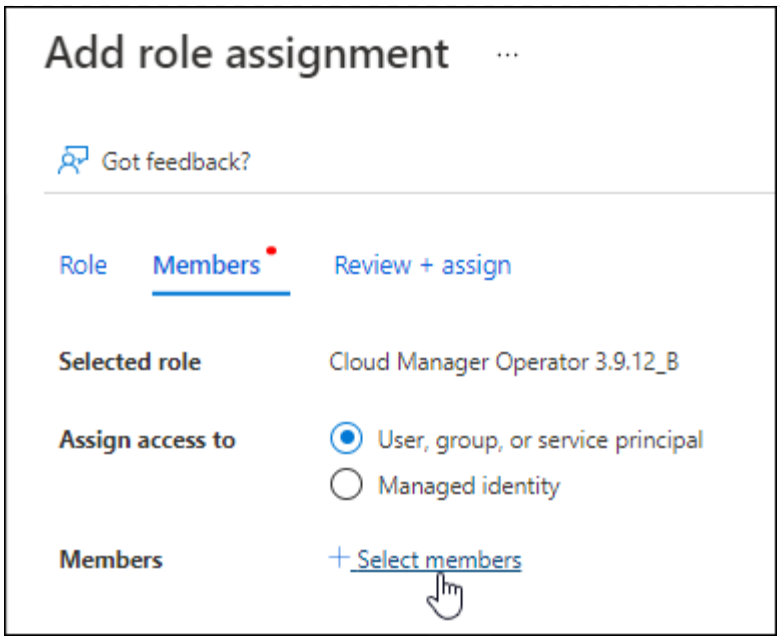
   b. Seleccione la suscripción.

   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**.

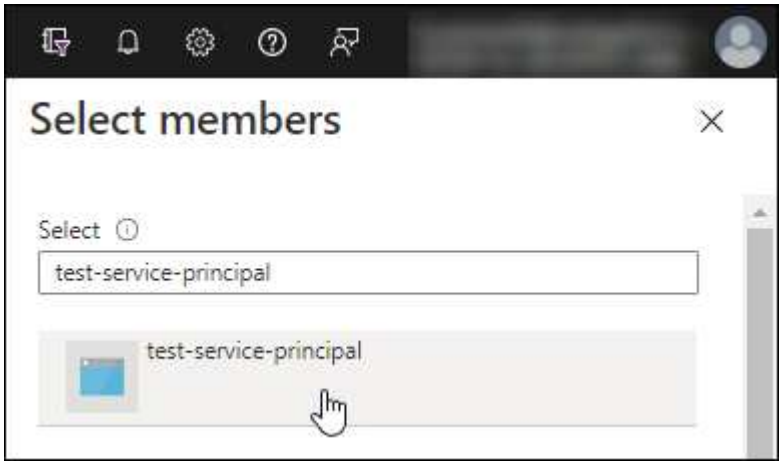
   e. En la pestaña **Miembros**, complete los siguientes pasos:

      - 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**.

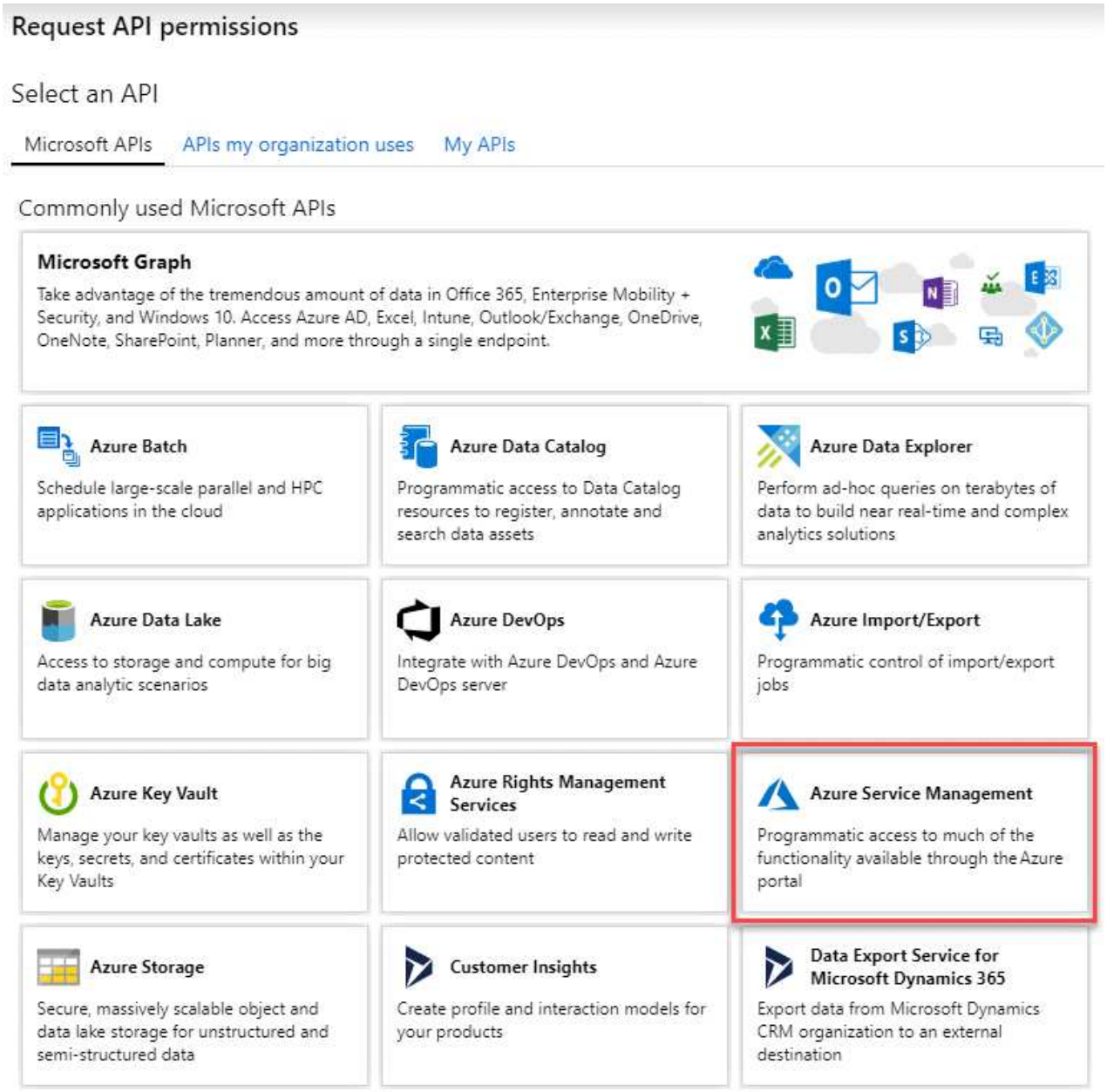
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

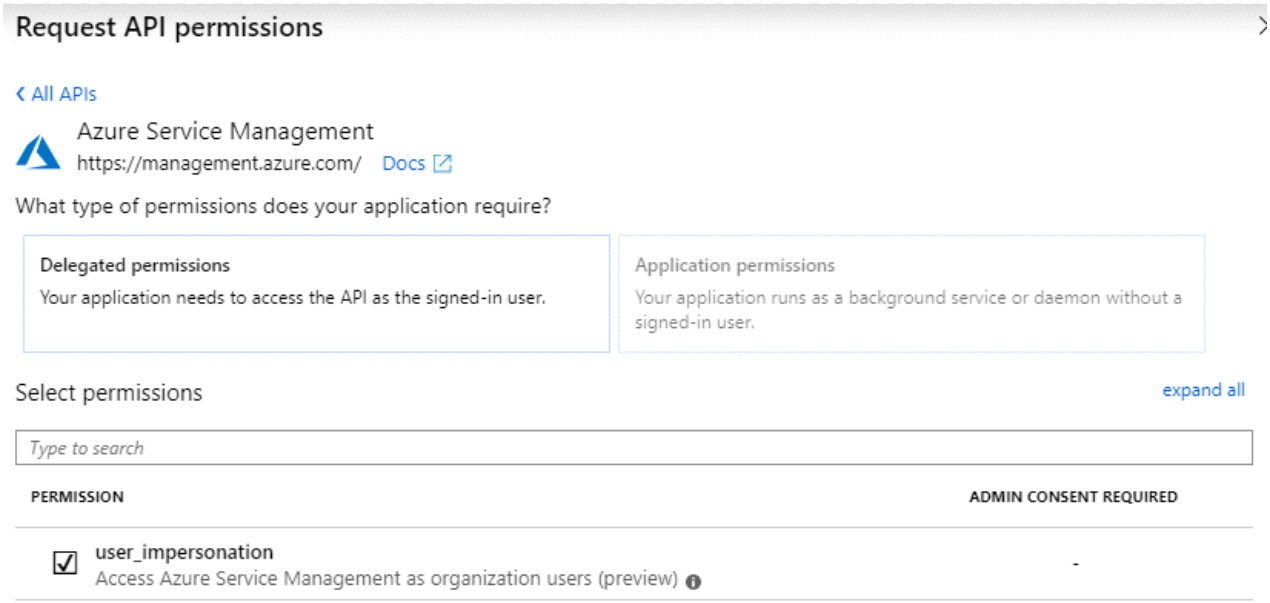
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

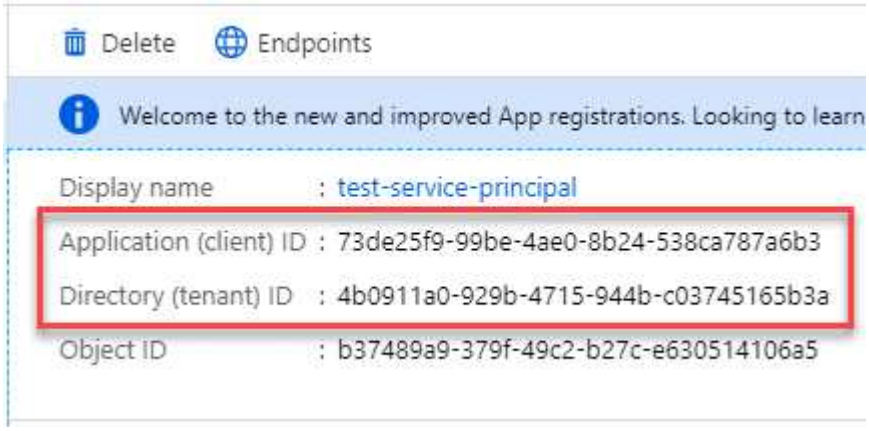


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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

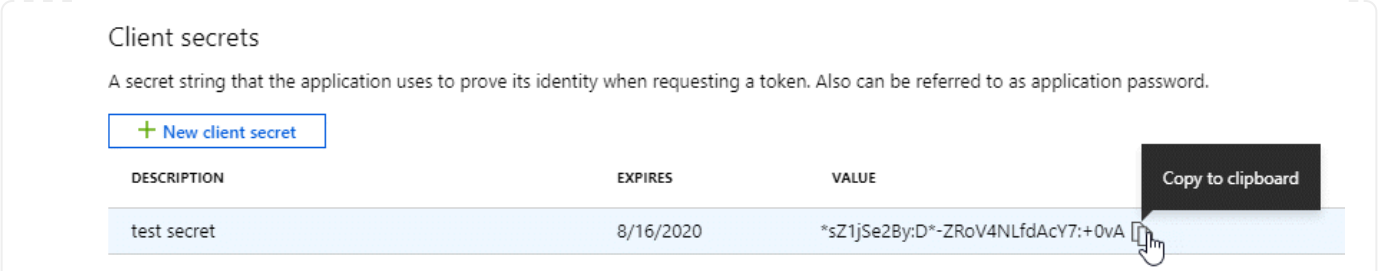
1. En el servicio **Microsoft Entra ID**, seleccione **Registros de aplicaciones** y seleccione la aplicación.
2. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)**.



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

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

"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 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
```

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

"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

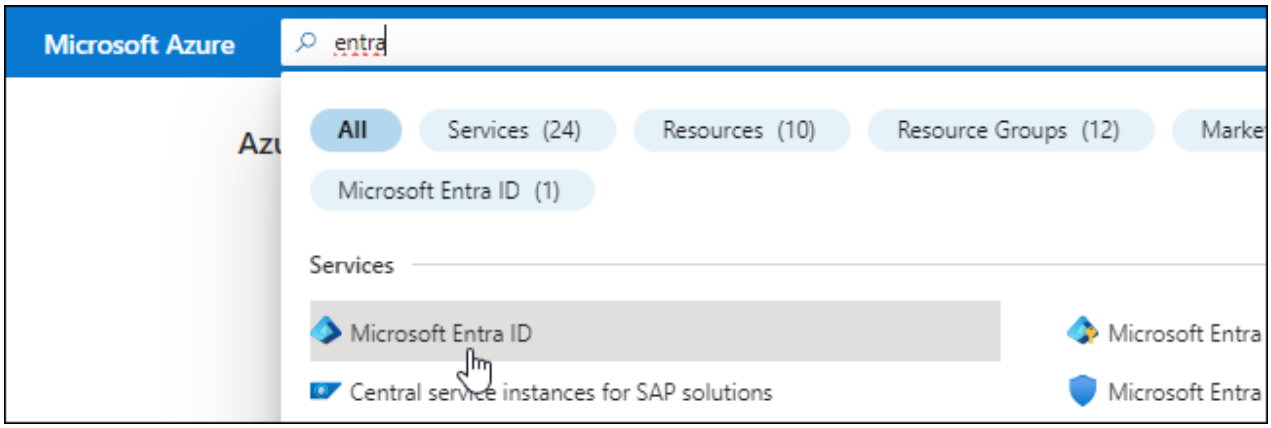
Cuando el agente de consola está instalado localmente, debe proporcionarle permisos de Azure configurando una entidad de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que necesita el agente de consola.

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 .

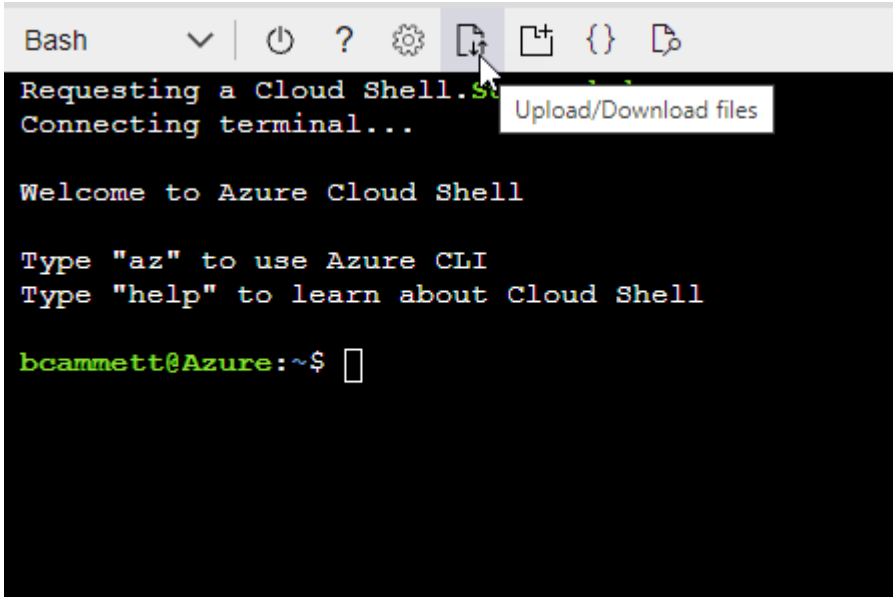
      Ejemplo

      ```
      "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:

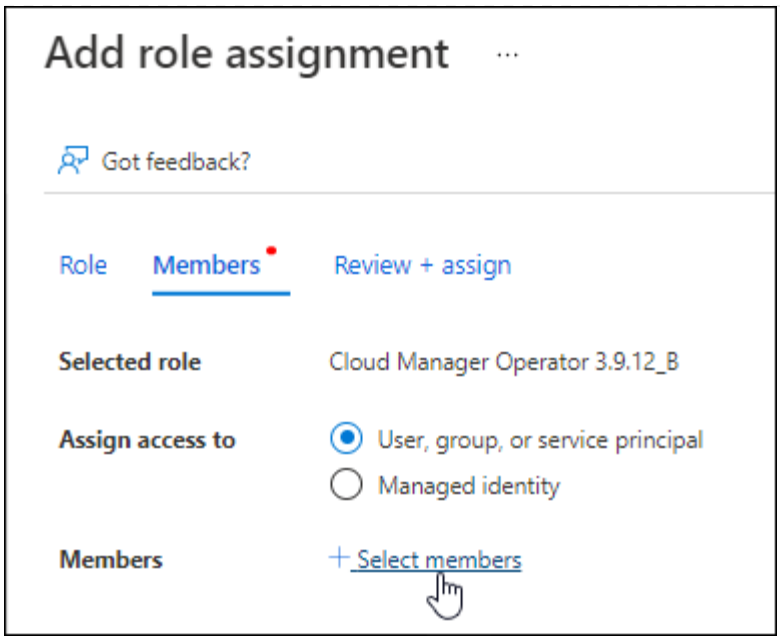
```
az role definition create --role-definition agent_Policy.json
```

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:

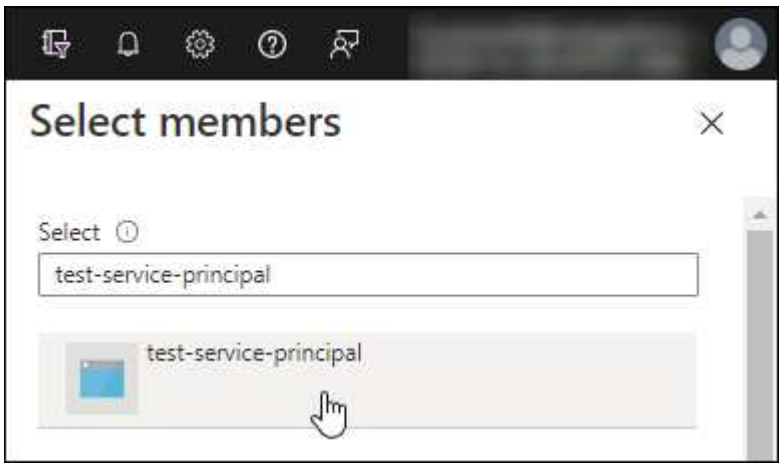
   a. Desde el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de rol**.
   d. En la pestaña **Rol**, seleccione el rol **Operador de consola** y seleccione **Siguiente**.
   e. En la pestaña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

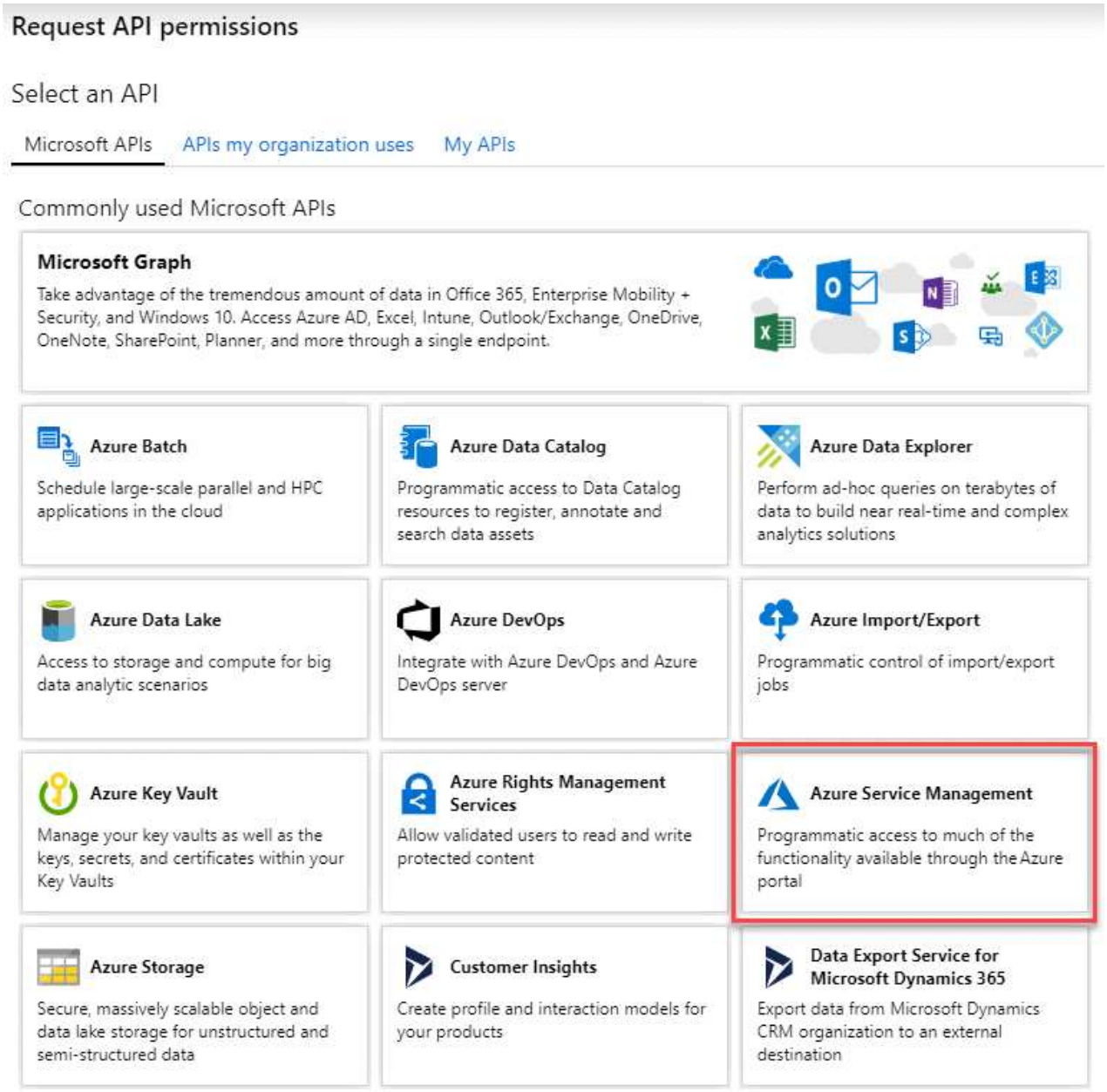
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

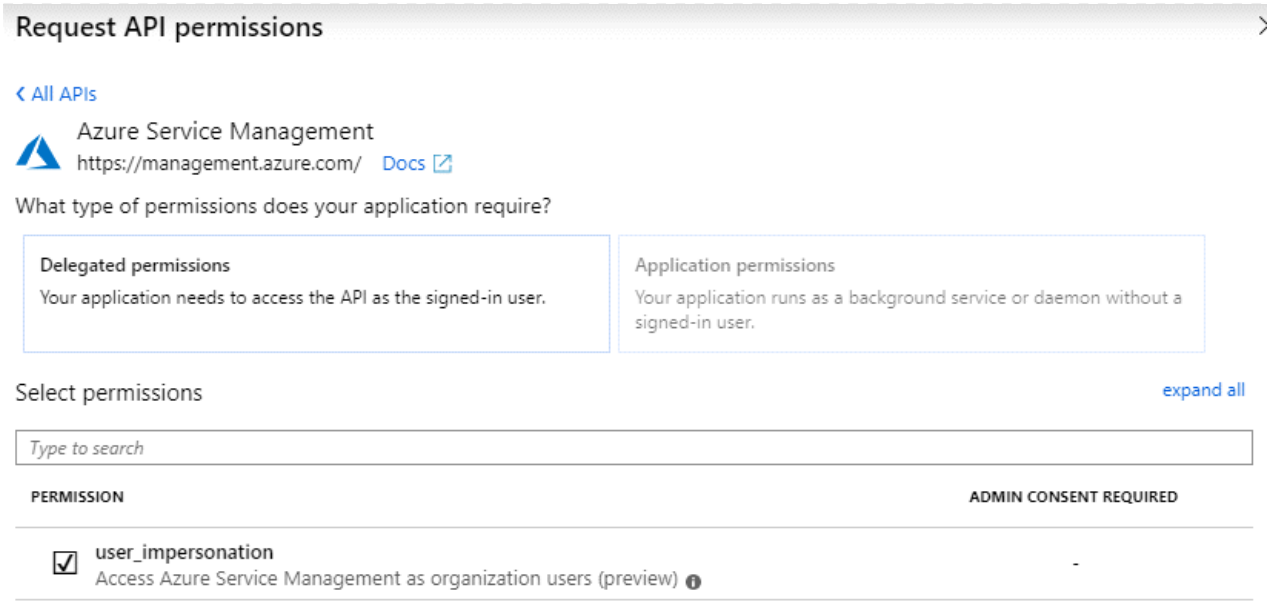
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

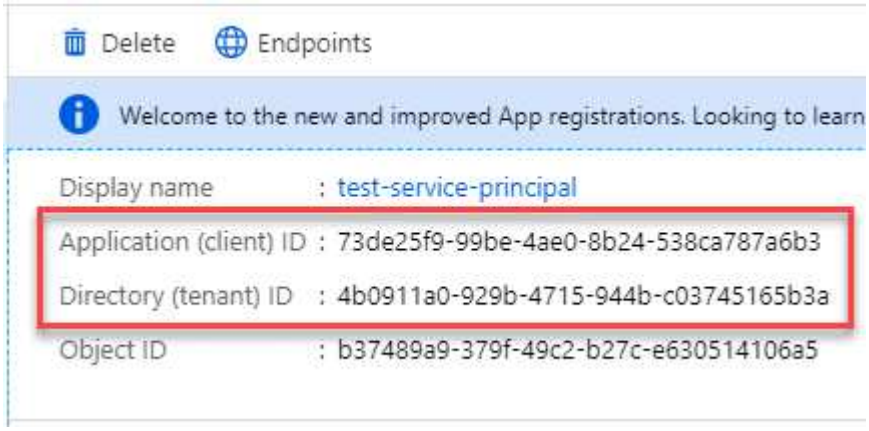


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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

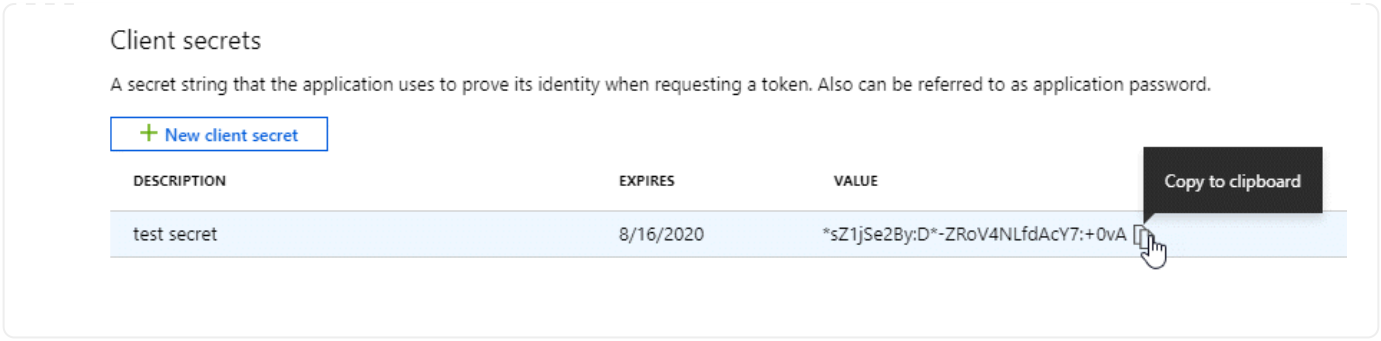
1. En el servicio **Microsoft Entra ID**, seleccione **Registros de aplicaciones** y seleccione la aplicación.
2. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)**.



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 5. 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

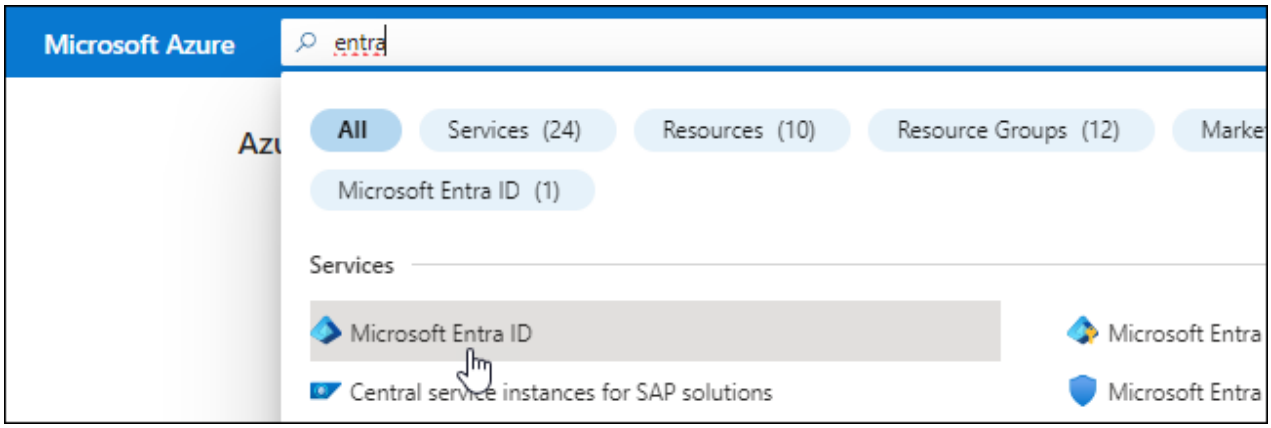
Cuando el agente de consola está instalado localmente, debe otorgarle permisos de Azure configurando una entidad de servicio en Microsoft Entra ID y obteniendo las credenciales de Azure que necesita el agente de consola.

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 .

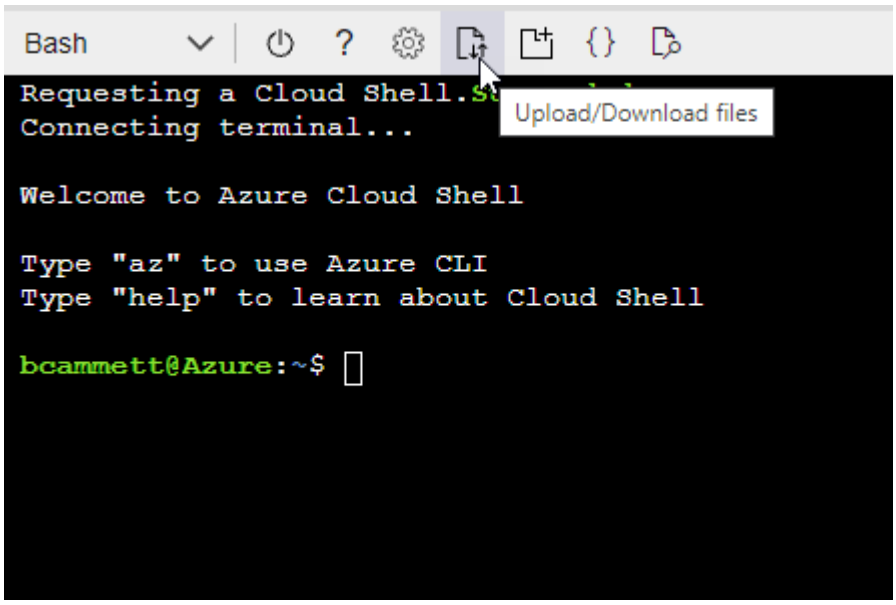
      Ejemplo

      ```
      "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:

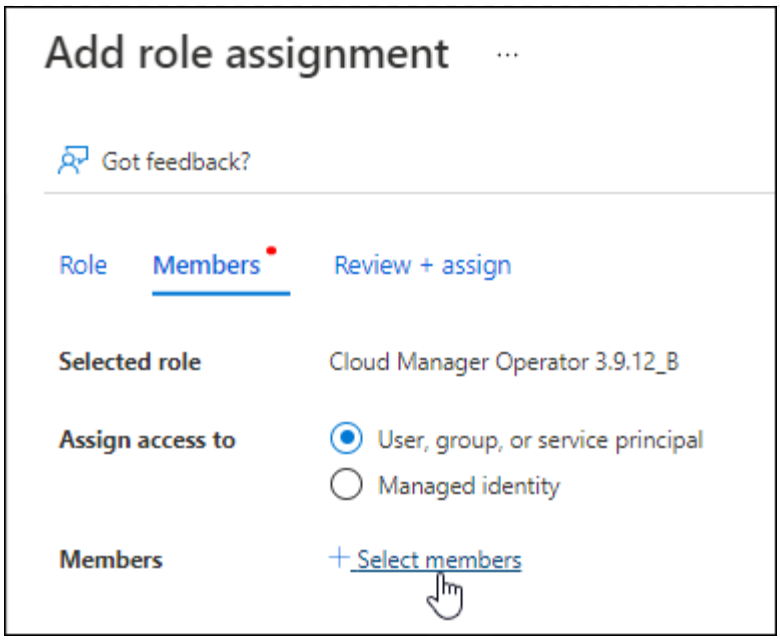
```
az role definition create --role-definition agent_Policy.json
```

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:

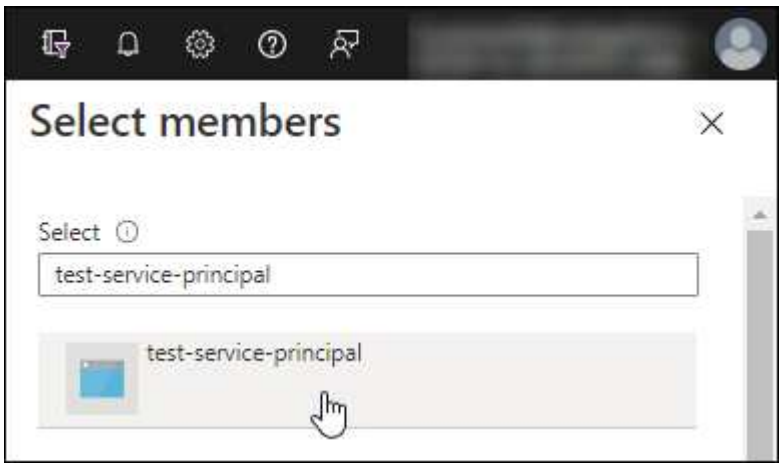
   a. Desde el portal de Azure, abra el servicio **Suscripciones**.
   b. Seleccione la suscripción.
   c. Seleccione **Control de acceso (IAM) > Agregar > Agregar asignación de rol**.
   d. En la pestaña **Rol**, seleccione el rol **Operador de consola** y seleccione **Siguiente**.
   e. En la pestaña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

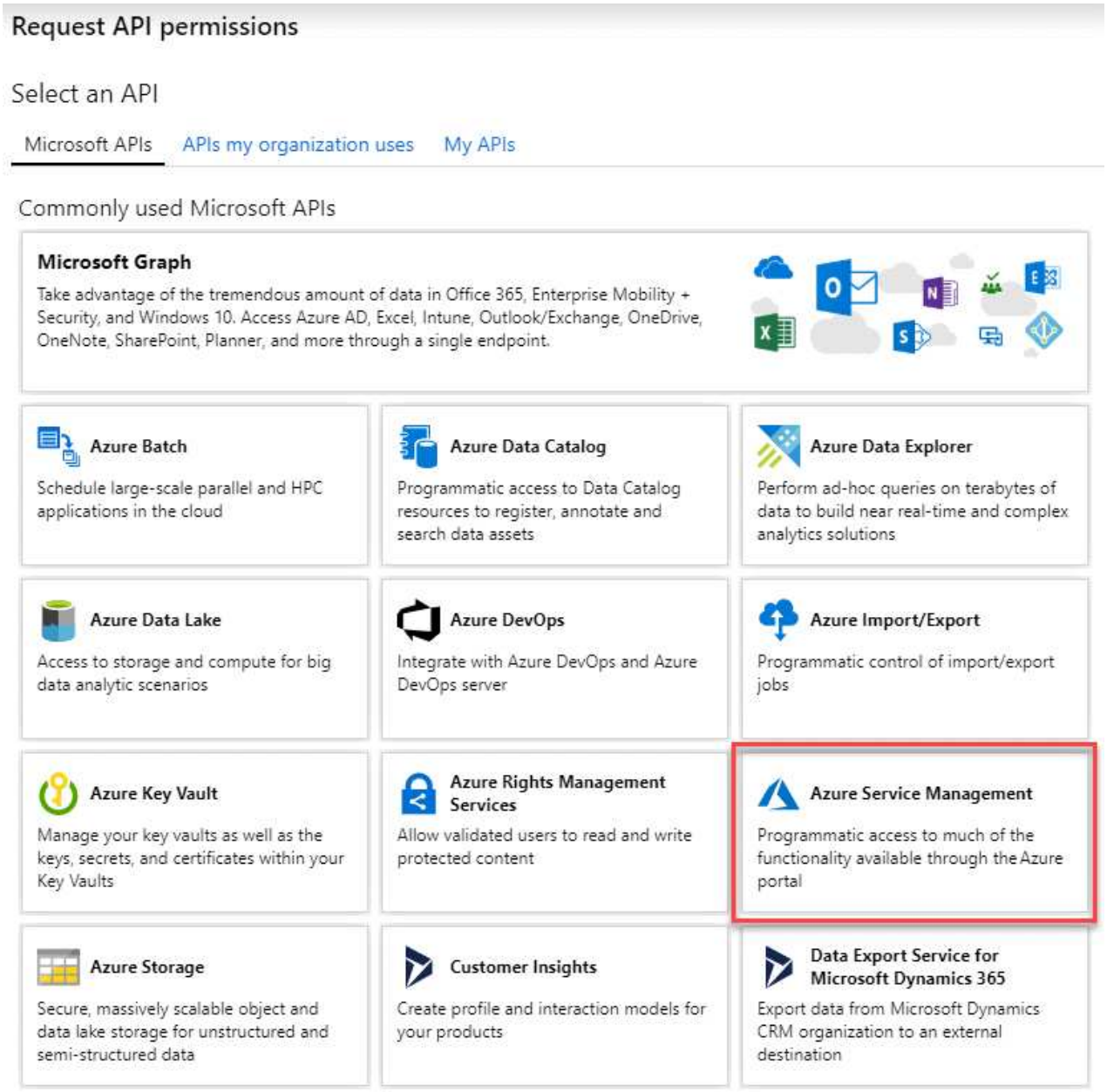
La entidad de servicio ahora tiene los permisos de Azure necesarios para implementar el agente de consola.

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.

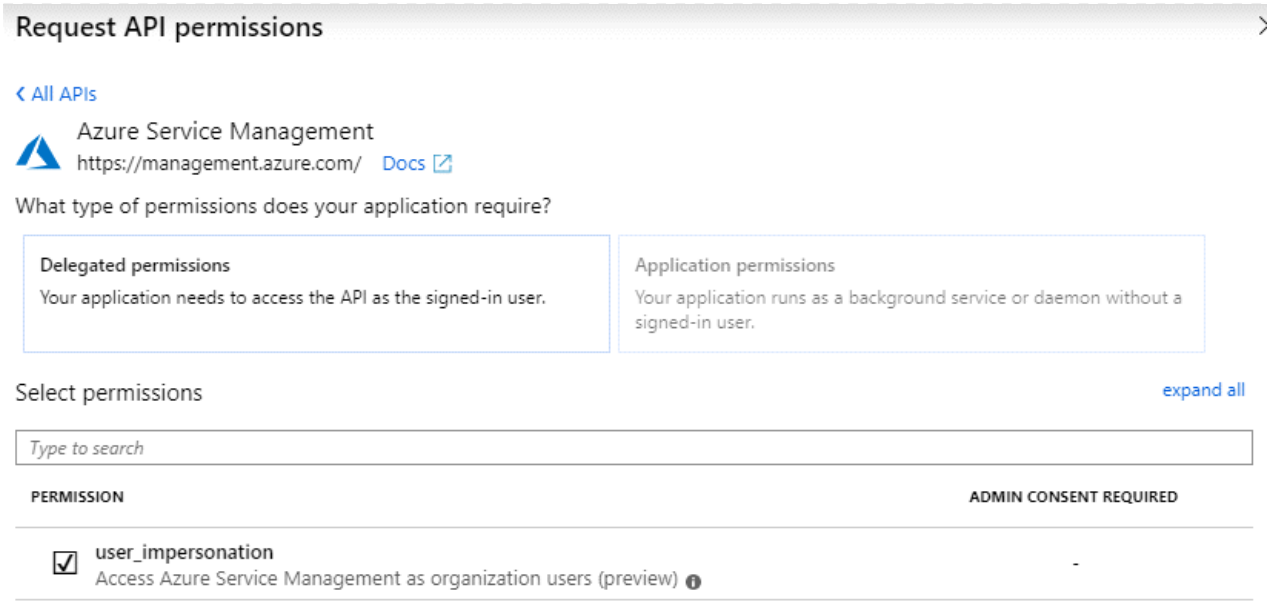
Agregar permisos de la API de administración de servicios de Windows Azure

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**.

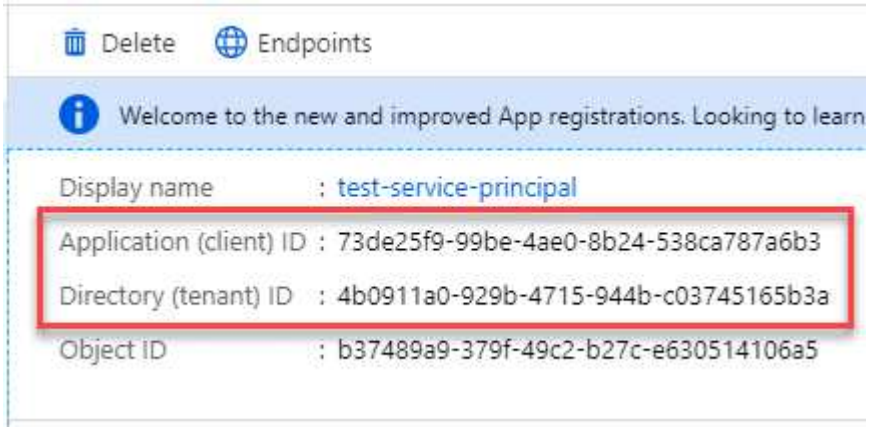


4. Seleccione **Acceder a Azure Service Management como usuarios de la organización** y luego seleccione **Agregar permisos**.



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

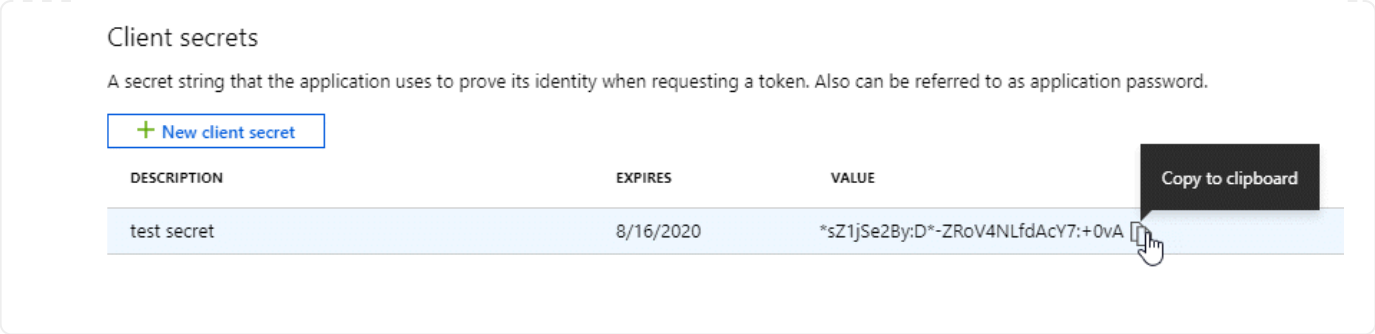
1. En el servicio **Microsoft Entra ID**, seleccione **Registros de aplicaciones** y seleccione la aplicación.
2. Copie el **ID de la aplicación (cliente)** y el **ID del directorio (inquilino)**.



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**.

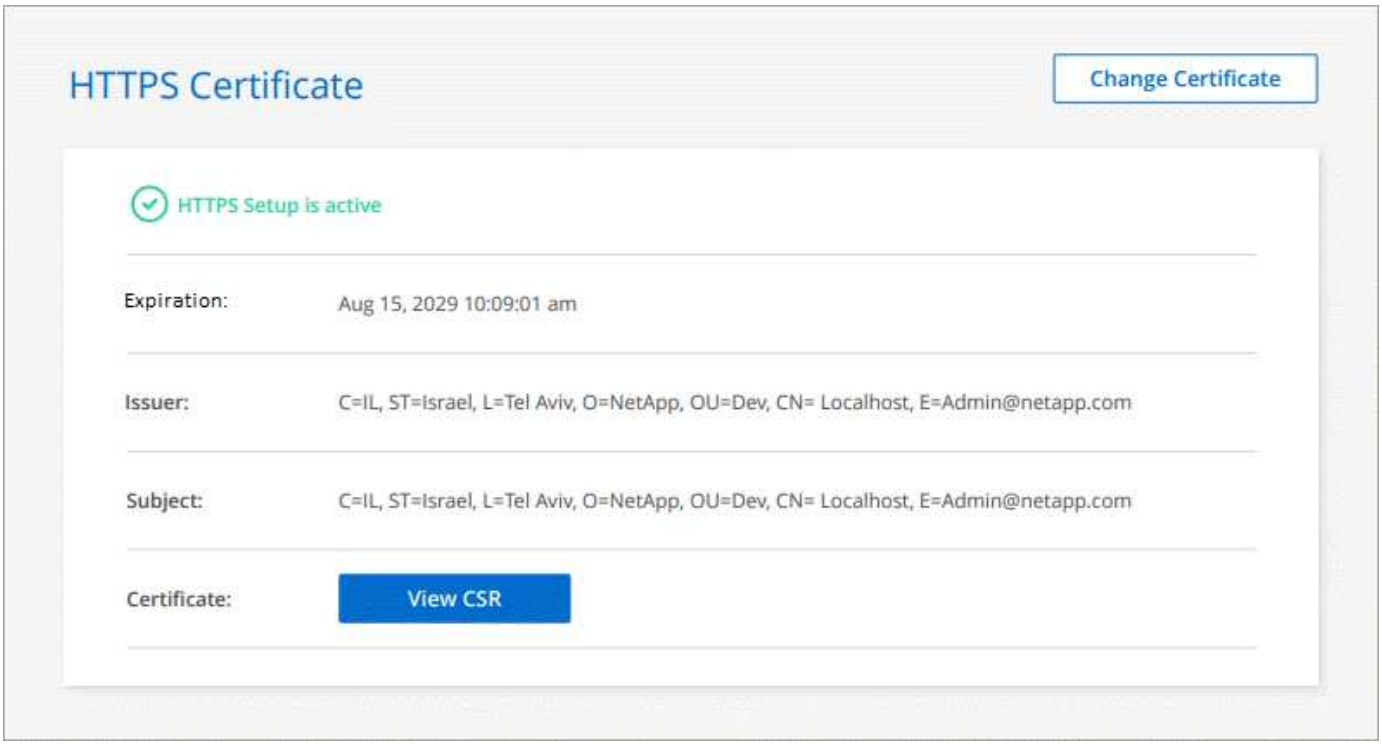
   El agente de la consola debe estar conectado para editarlo.

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

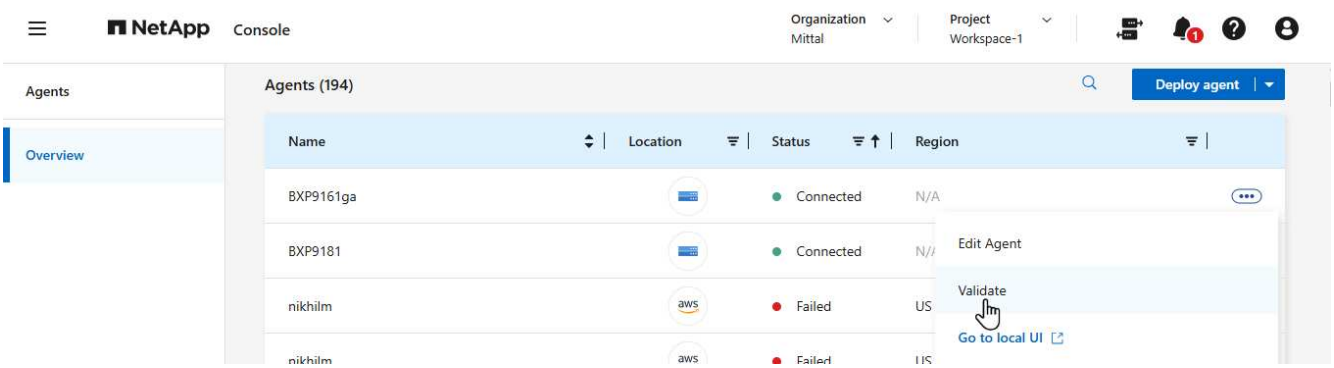
Ejecute comprobaciones de configuración en los agentes de la consola desde la consola o desde la consola de mantenimiento del agente para asegurarse de que estén conectados.

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

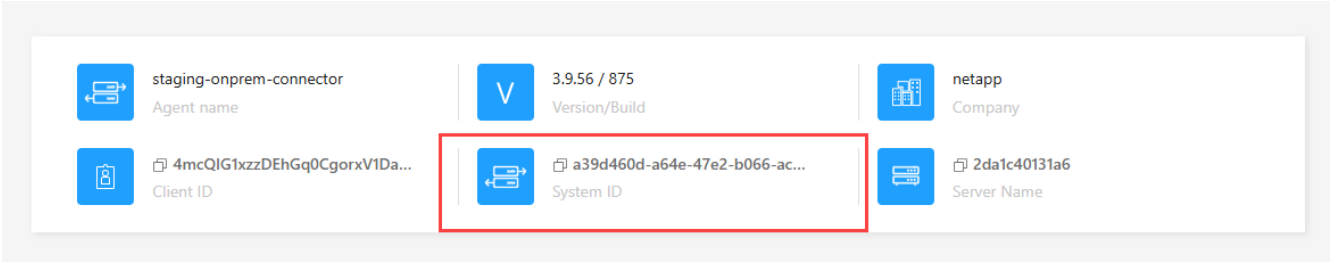
Para ayudarlo a comenzar, es posible que necesite el ID del sistema de su agente de consola. La identificación normalmente se utiliza para fines de licencia y resolución de problemas.

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

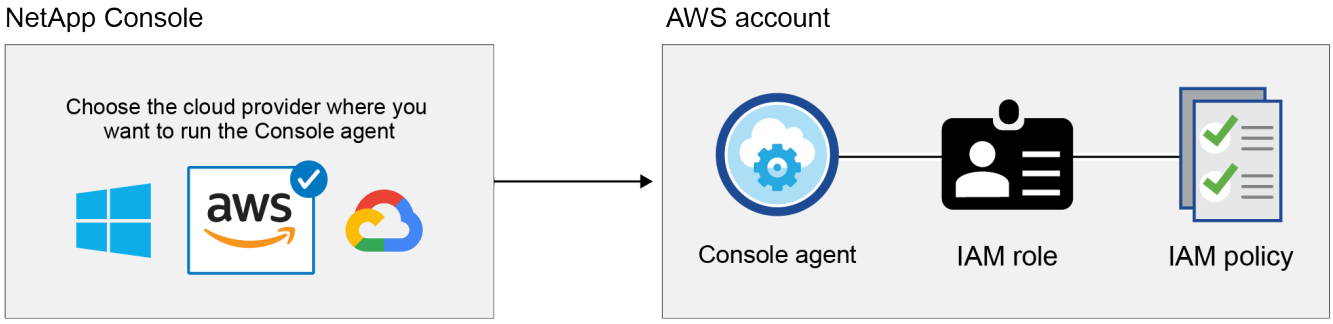
Obtenga información sobre las credenciales y los permisos de AWS en la NetApp Console

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.

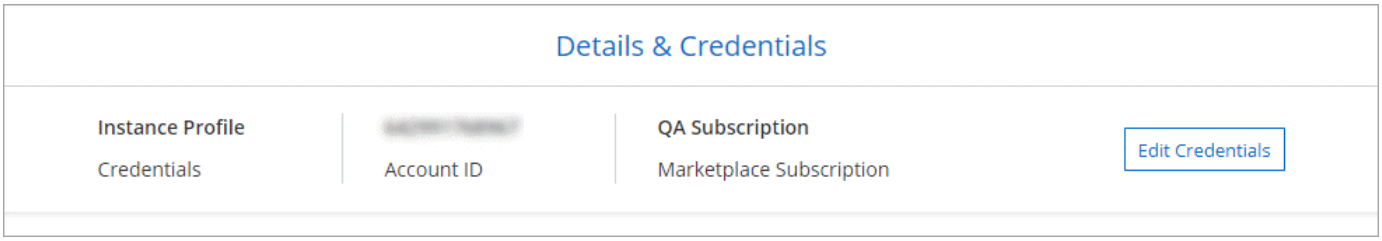
Credenciales iniciales de AWS

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

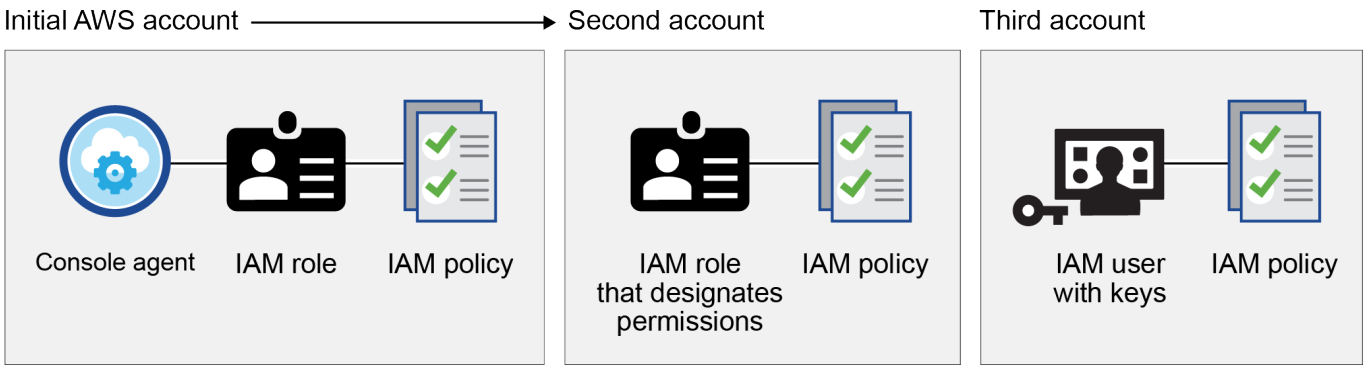
Puede agregar credenciales de AWS adicionales a la consola en los siguientes casos:

- 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.

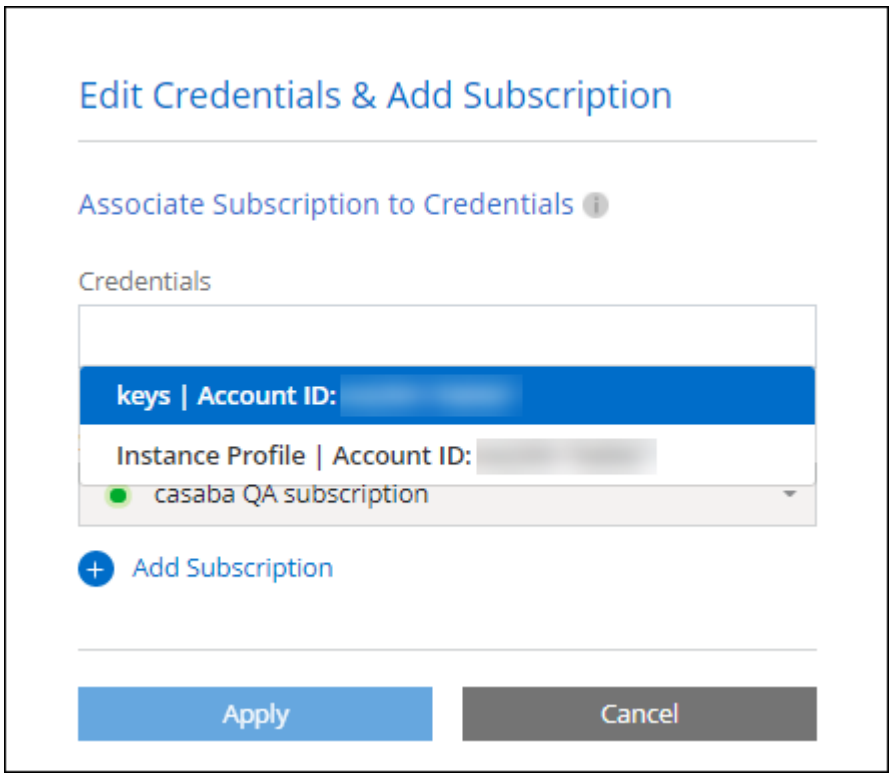
Agregue credenciales de AWS para usar un agente de consola con otra cuenta de AWS

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

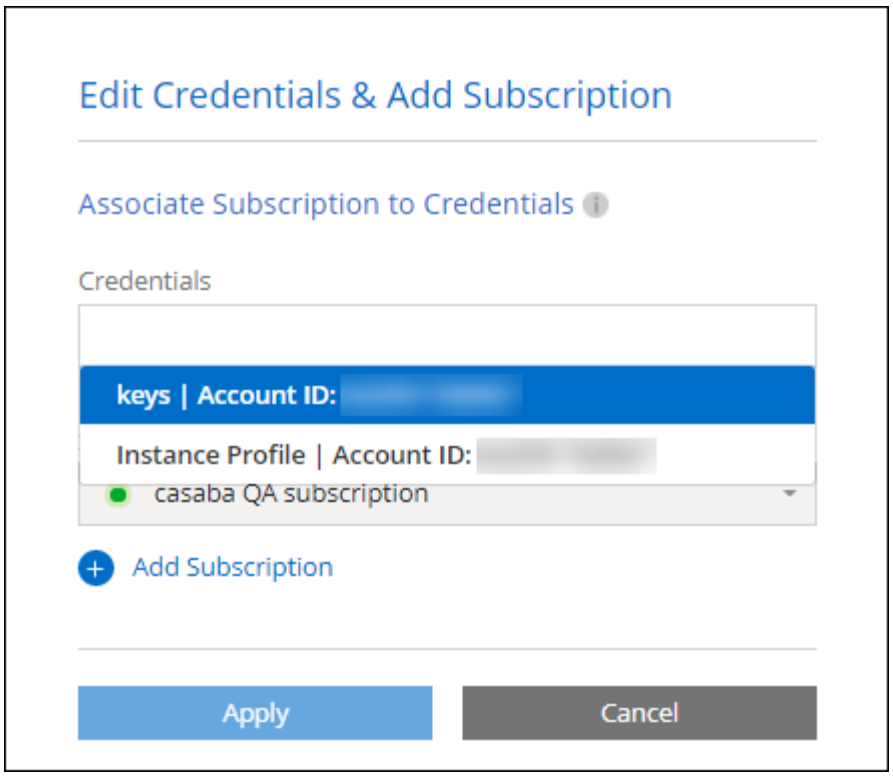
1. Utilice la barra de navegación superior para seleccionar un agente de consola al que desea agregar credenciales.
2. En la barra de navegación izquierda, seleccione **Administración > Credenciales**.
3. En la página **Credenciales de la organización**, seleccione **Agregar credenciales** y siga los 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

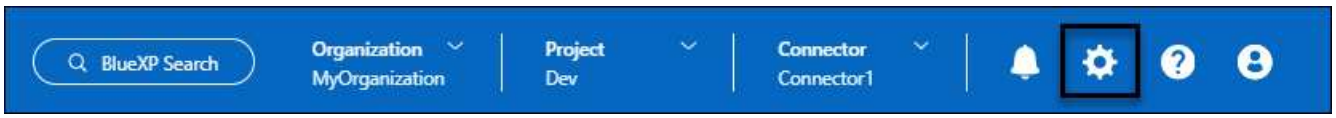
Después de proporcionar al rol IAM los permisos necesarios, agregue el ARN del rol a la consola.

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.

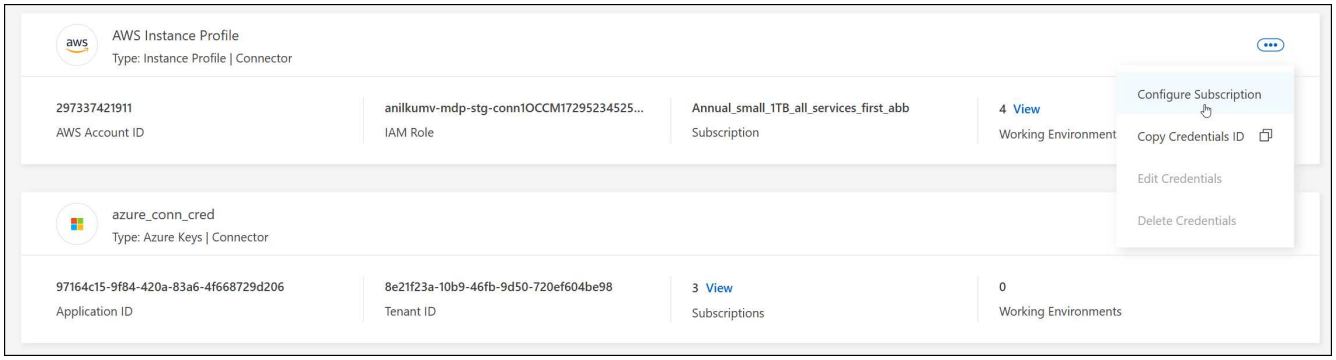
Antes de empezar

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.

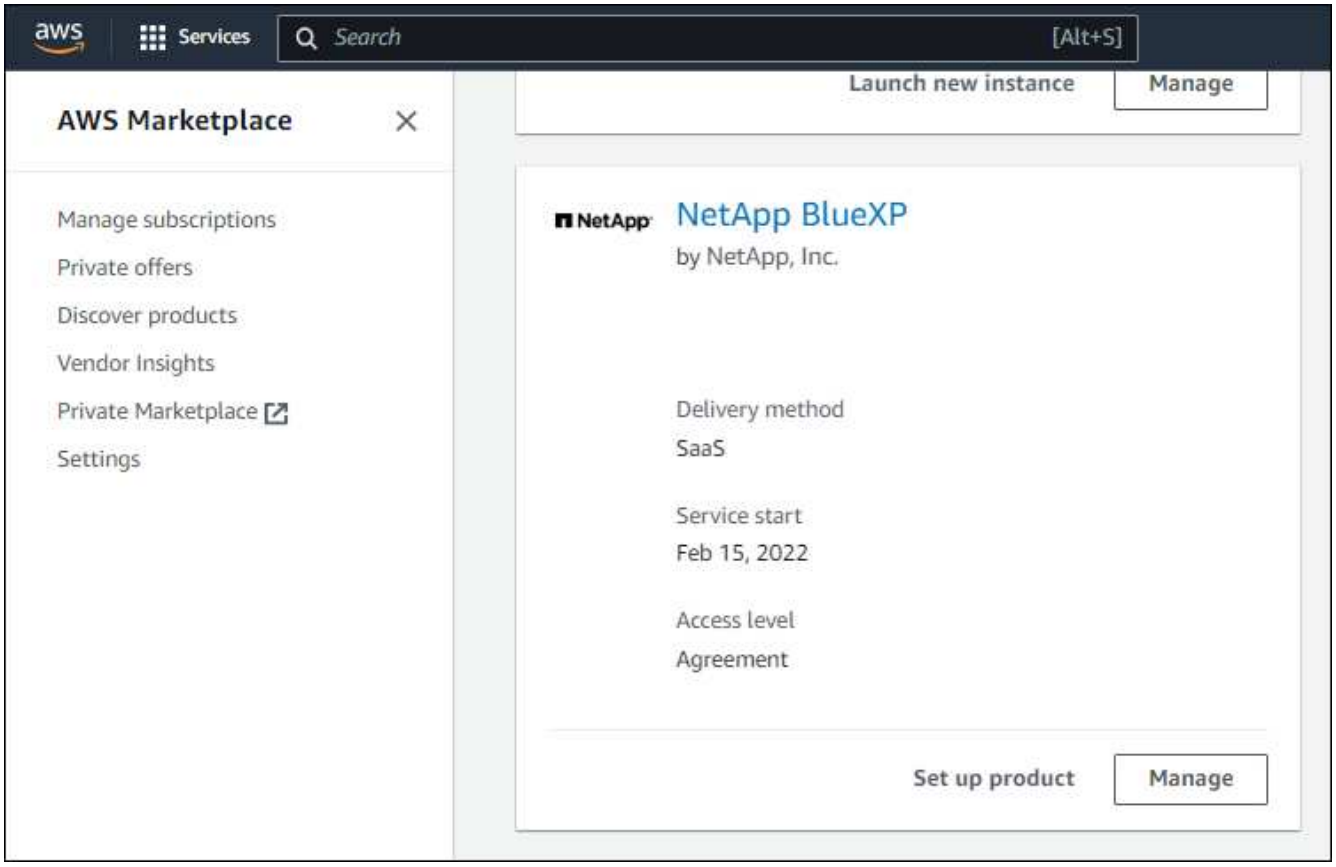
- "Obtenga más información sobre los modos de implementación de la consola"
- "Obtenga más información sobre la gestión de identidad y acceso de la consola"

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.

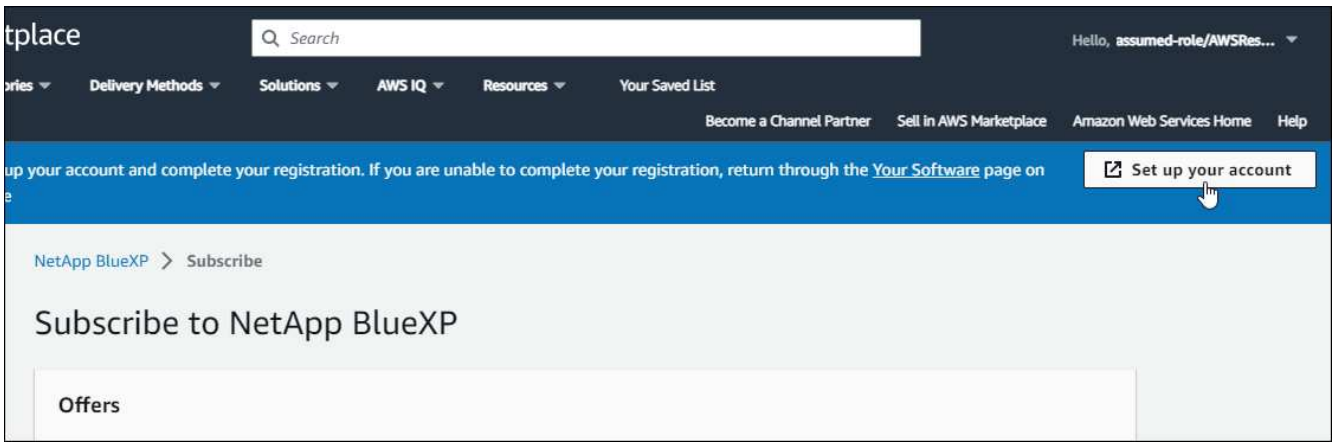
      Solo verás las suscripciones asociadas con la organización o cuenta que estás viendo actualmente. Si no ve su suscripción, continúe con los siguientes pasos.
2. Inicie sesión en la consola de AWS y navegue a **Suscripciones de AWS Marketplace**.
3. Encuentra la suscripción.



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.

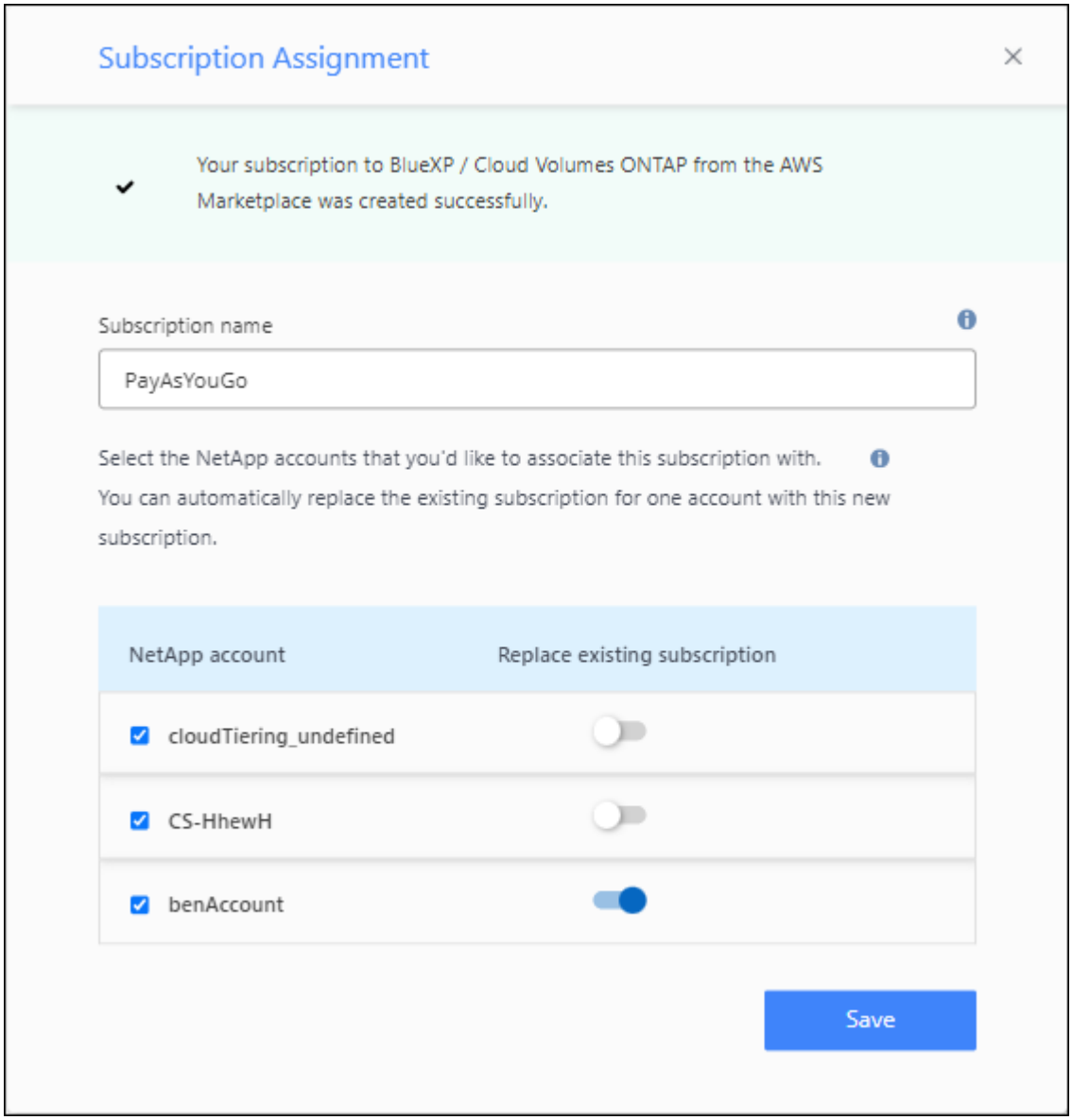
6. Desde la página **Asignación de suscripción**:

   - 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.

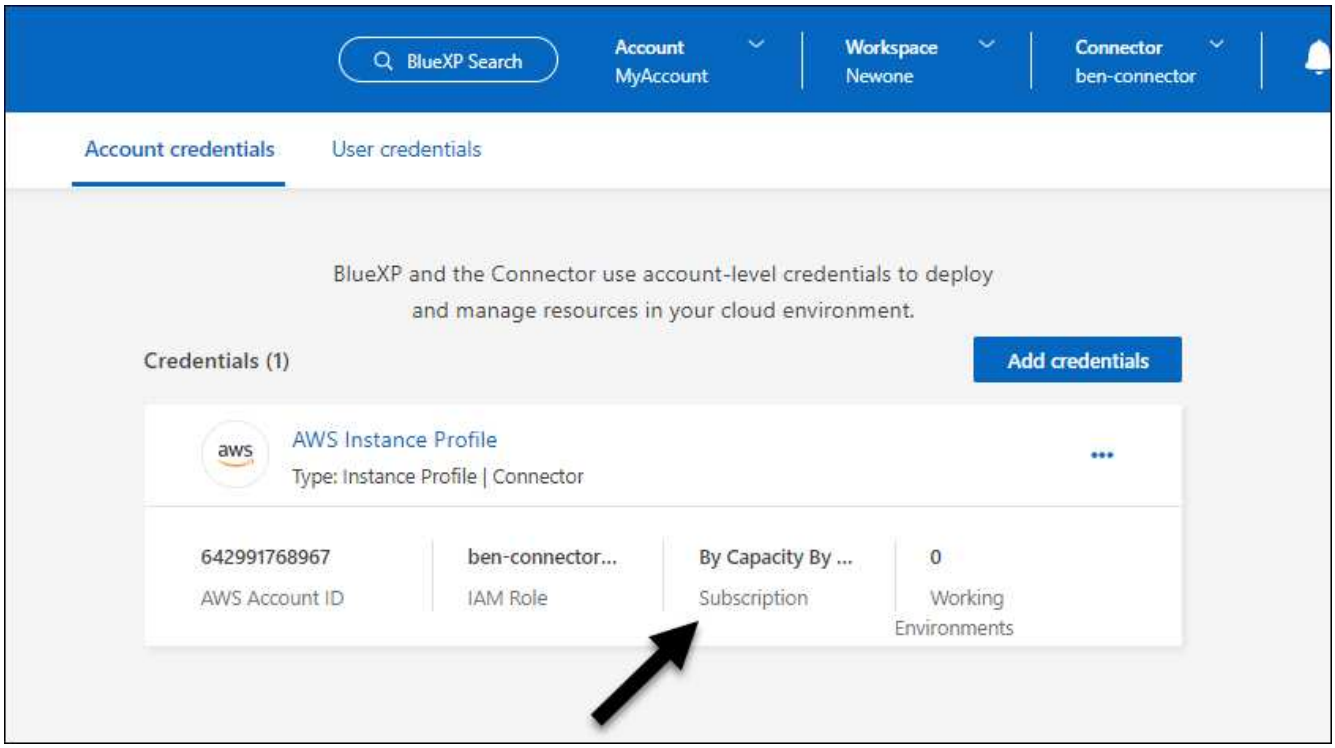
  Para todas las demás organizaciones o cuentas, deberá asociar manualmente la suscripción repitiendo estos pasos.



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

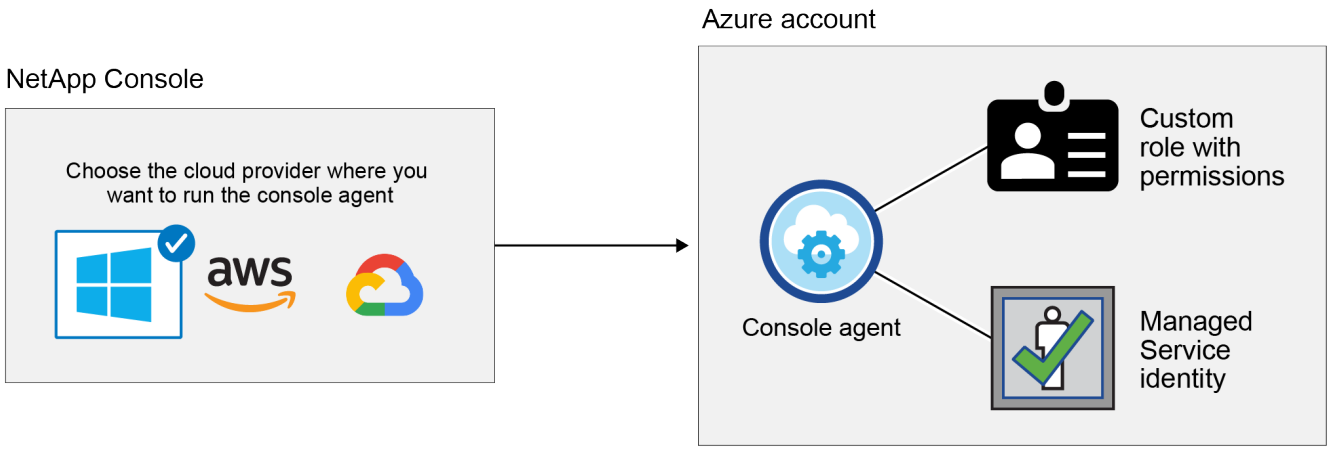
Obtenga información sobre las credenciales y los permisos de Azure en la NetApp Console

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.

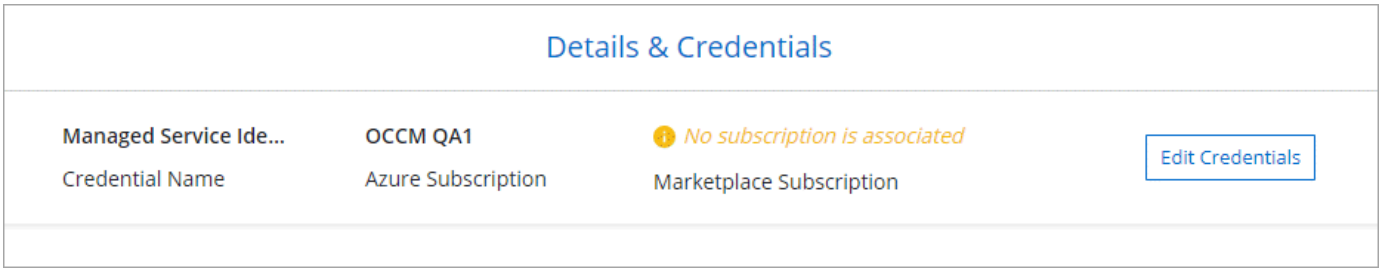
Credenciales iniciales de Azure

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:



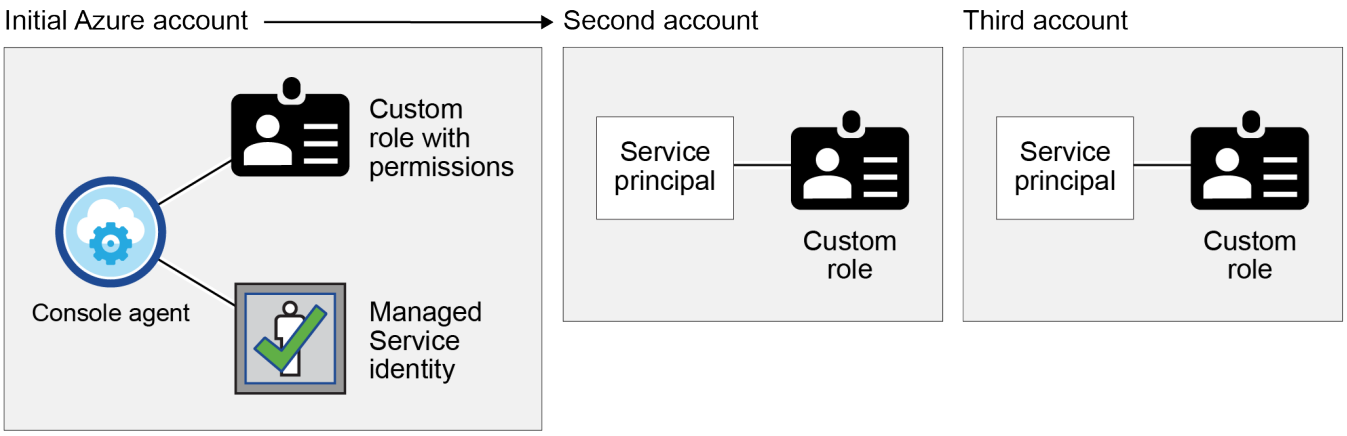
Puede implementar todos sus sistemas Cloud Volumes ONTAP utilizando las credenciales iniciales de Azure o puede agregar credenciales adicionales.

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" .

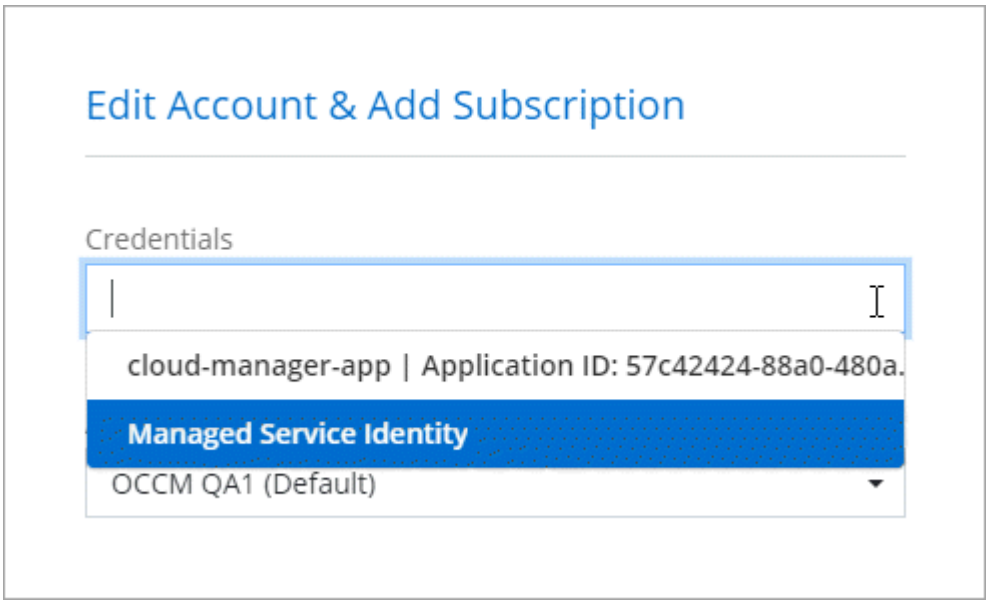
Credenciales adicionales de Azure

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.

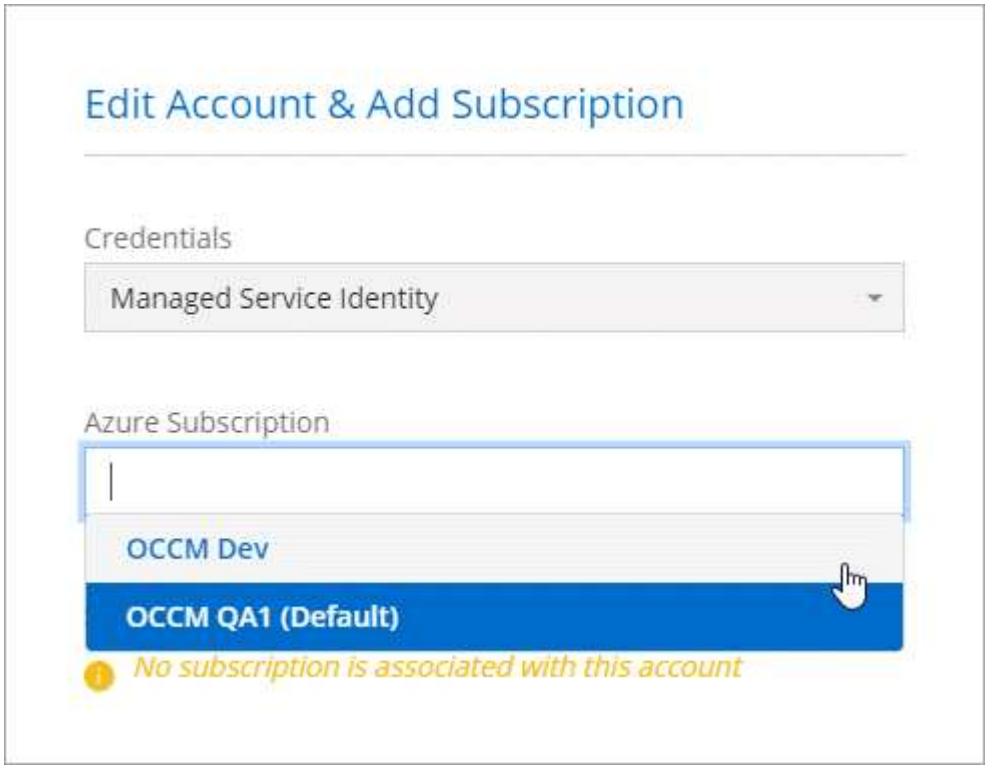
      - Asignar acceso a una **Máquina Virtual**.
      - Seleccione la suscripción en la que se creó una máquina virtual del agente de consola.
      - Seleccione una máquina virtual del agente de consola.

- 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.

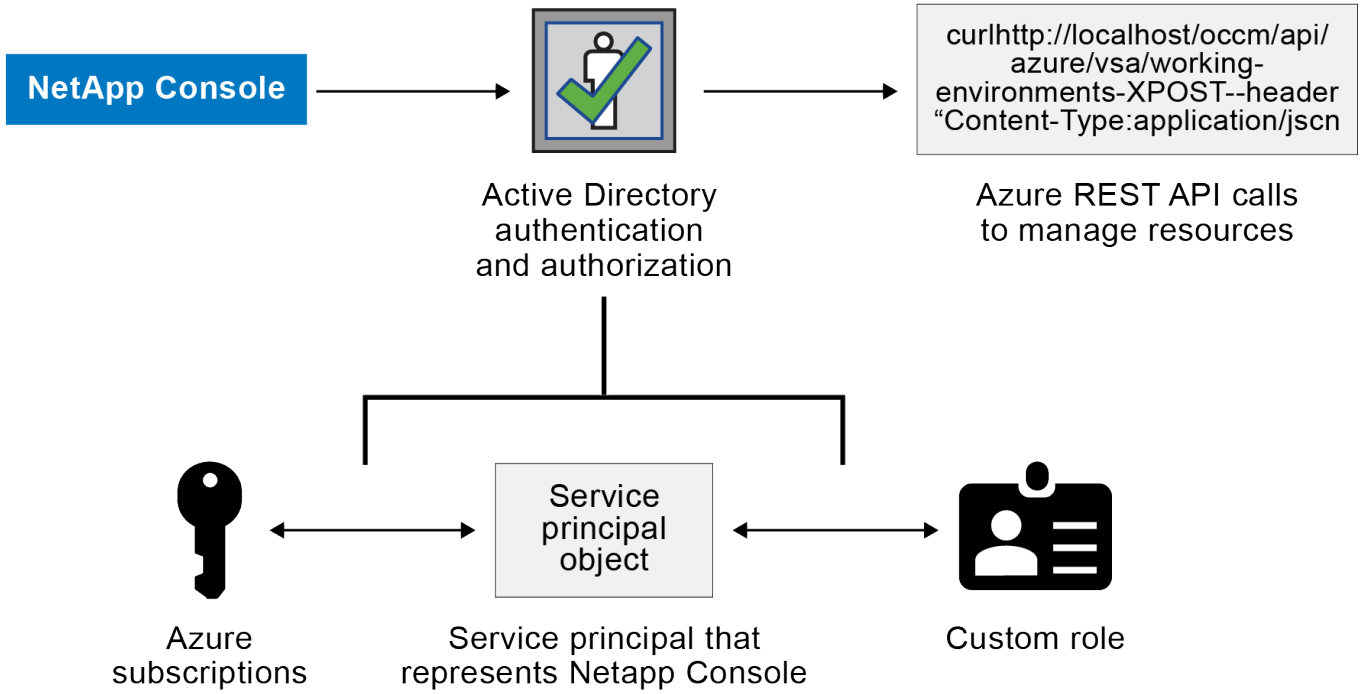
Otorgar permisos de Azure mediante una entidad de servicio

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

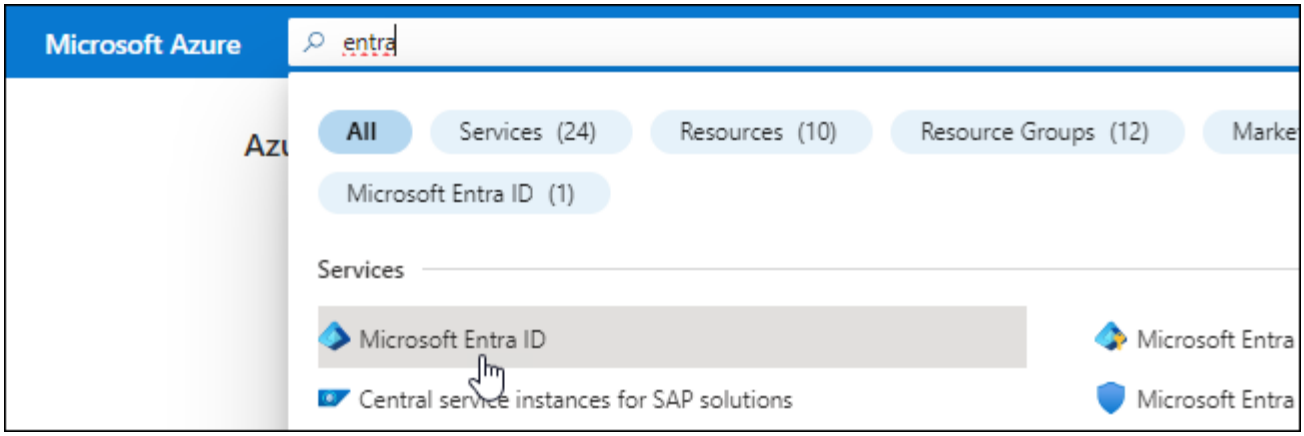
Cree una aplicación Microsoft Entra y una entidad de servicio que la consola pueda usar para el control de acceso basado en roles.

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 .

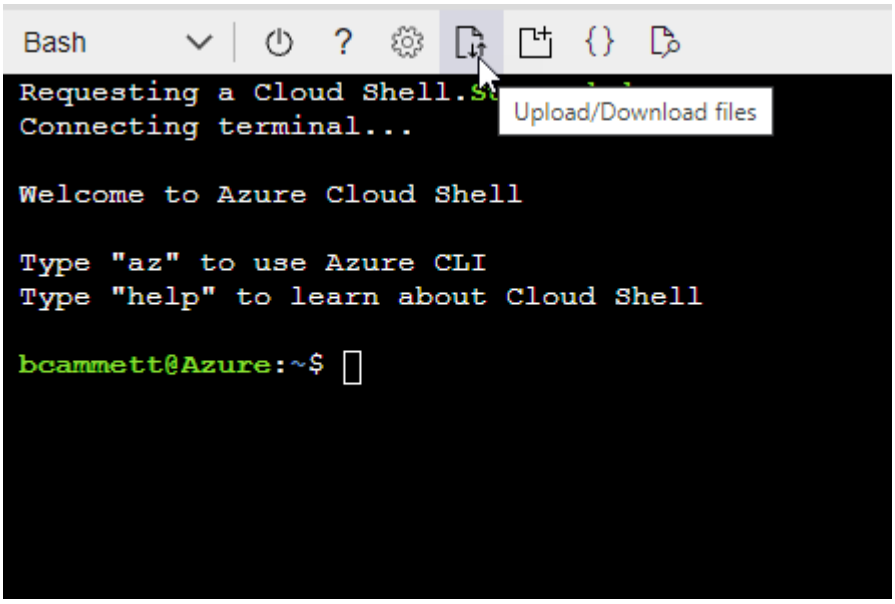
      Ejemplo

```
"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
```

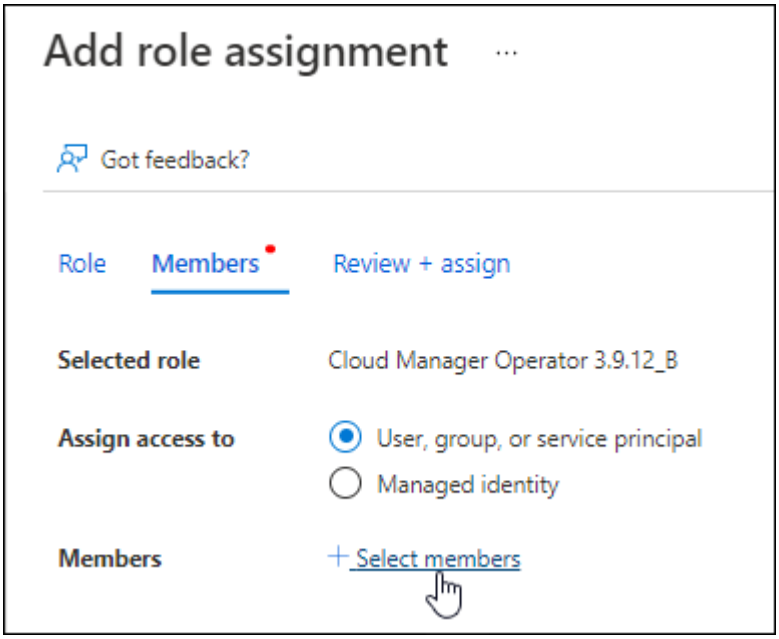
Ahora debería tener un rol personalizado llamado Operador de consola que puede asignar a la máquina virtual del agente de consola.

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:

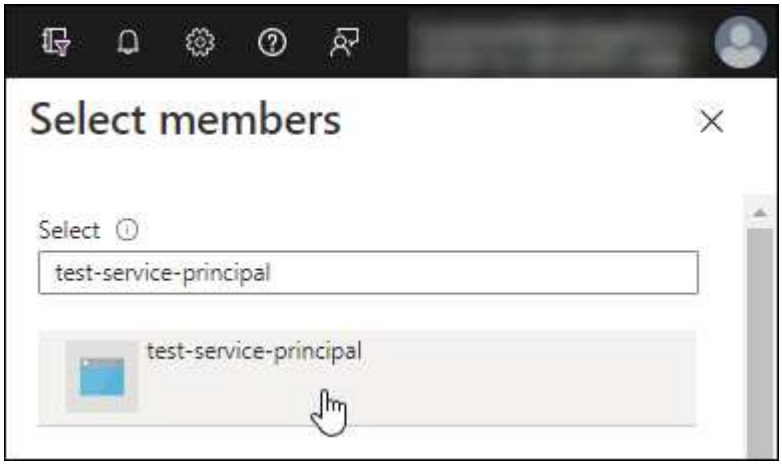
- Mantenga seleccionado **Usuario, grupo o entidad de servicio**.

- 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.

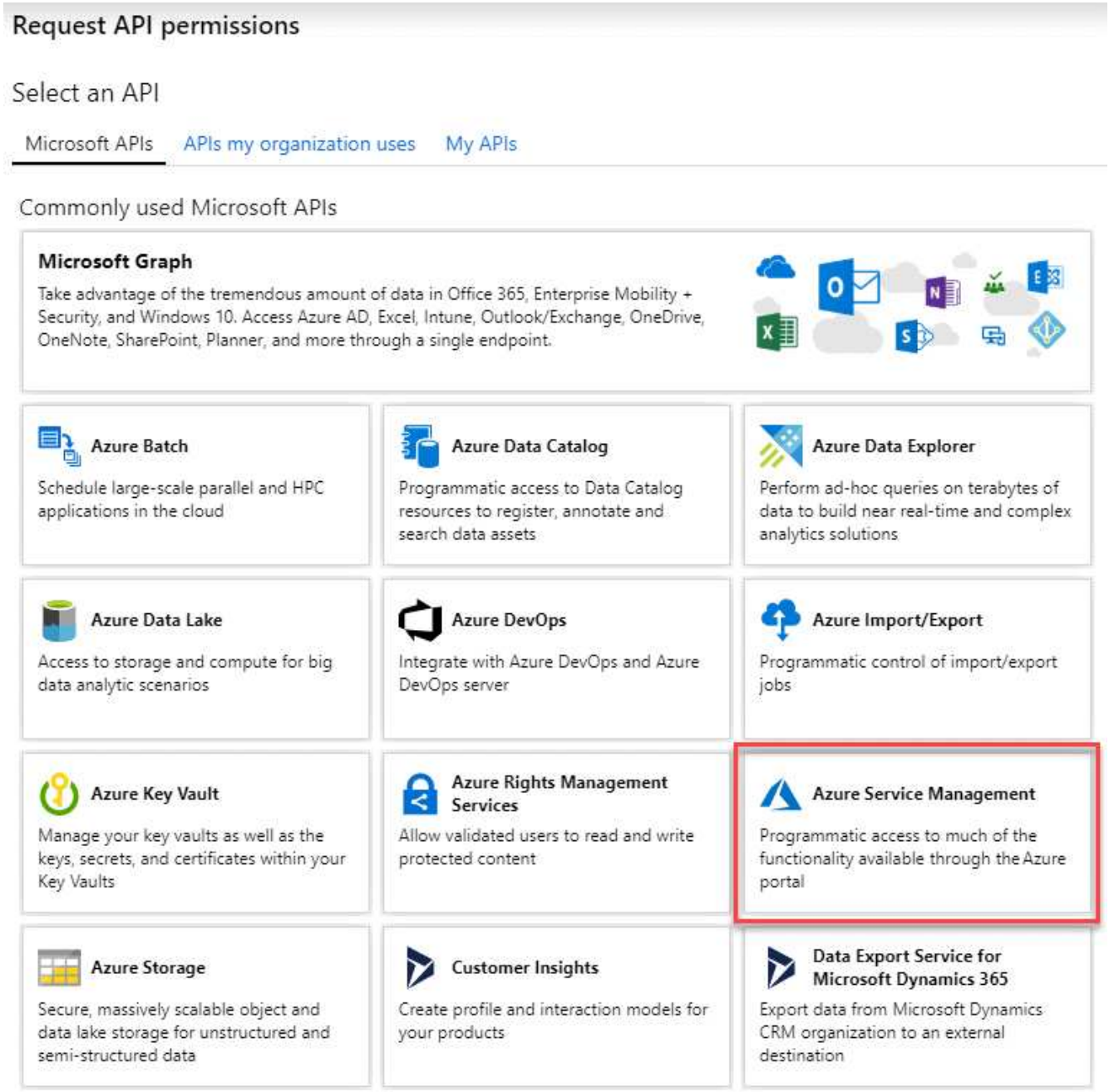
Si desea implementar Cloud Volumes ONTAP desde varias suscripciones de Azure, debe vincular la entidad de servicio a cada una de esas suscripciones. En la NetApp Console, puede seleccionar la suscripción que desea utilizar al implementar Cloud Volumes ONTAP.

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

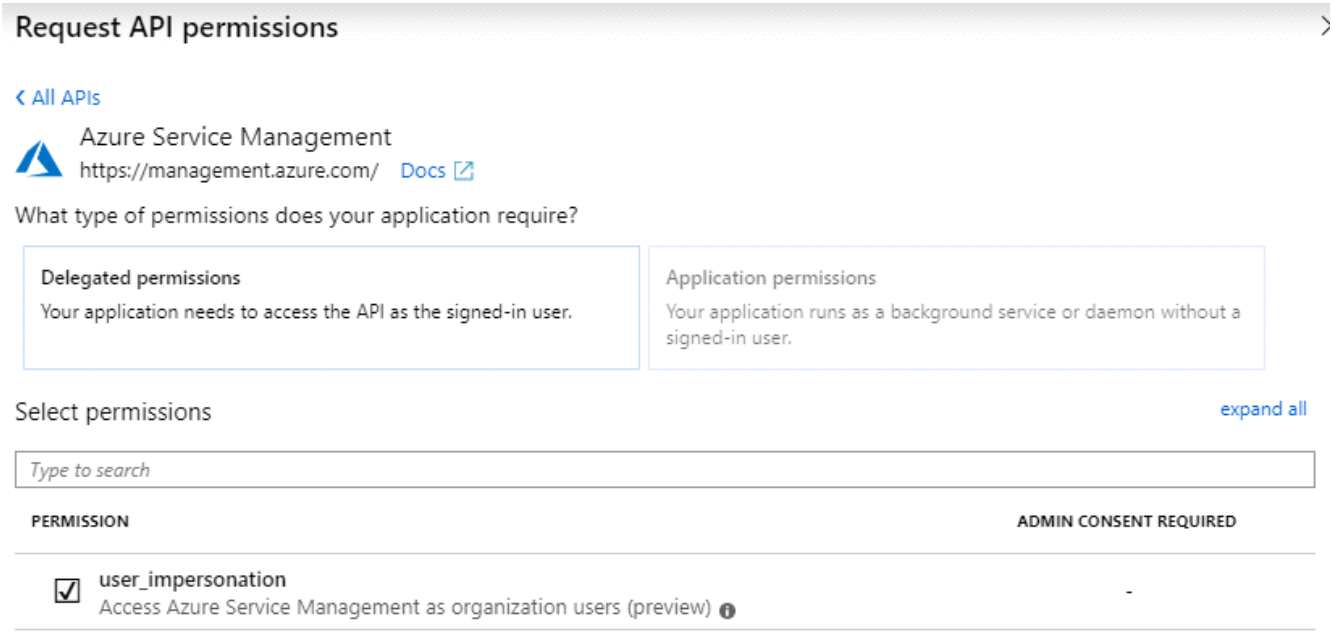
Debe asignar permisos de "API de administración de servicios de Windows Azure" a la entidad de servicio.

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**.

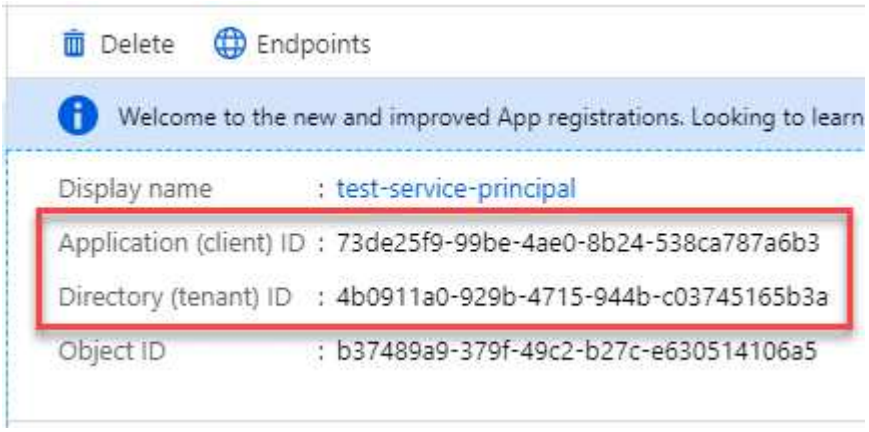


Obtener el ID de la aplicación y el ID del directorio

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" .

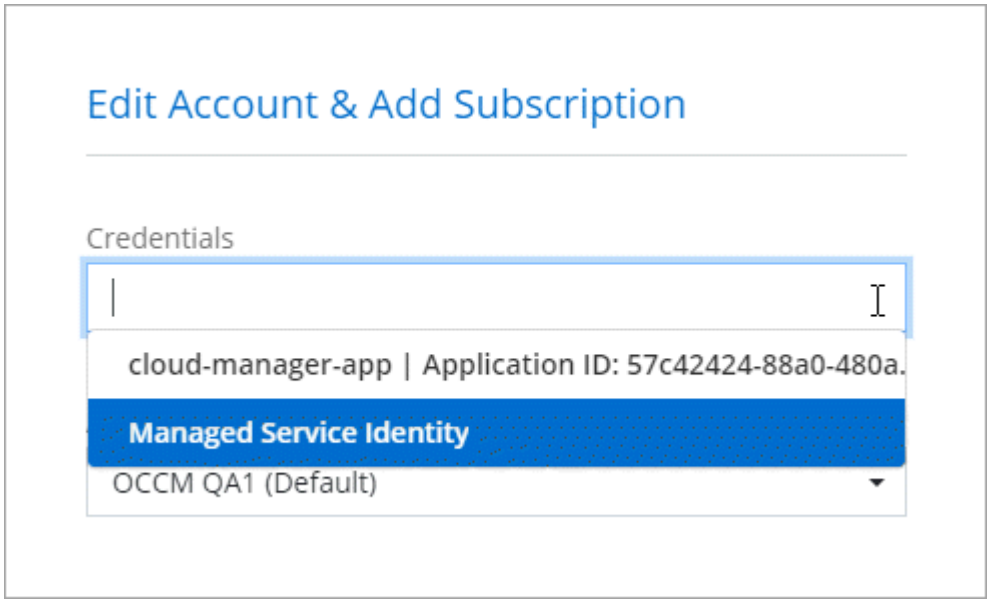
Pasos

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.

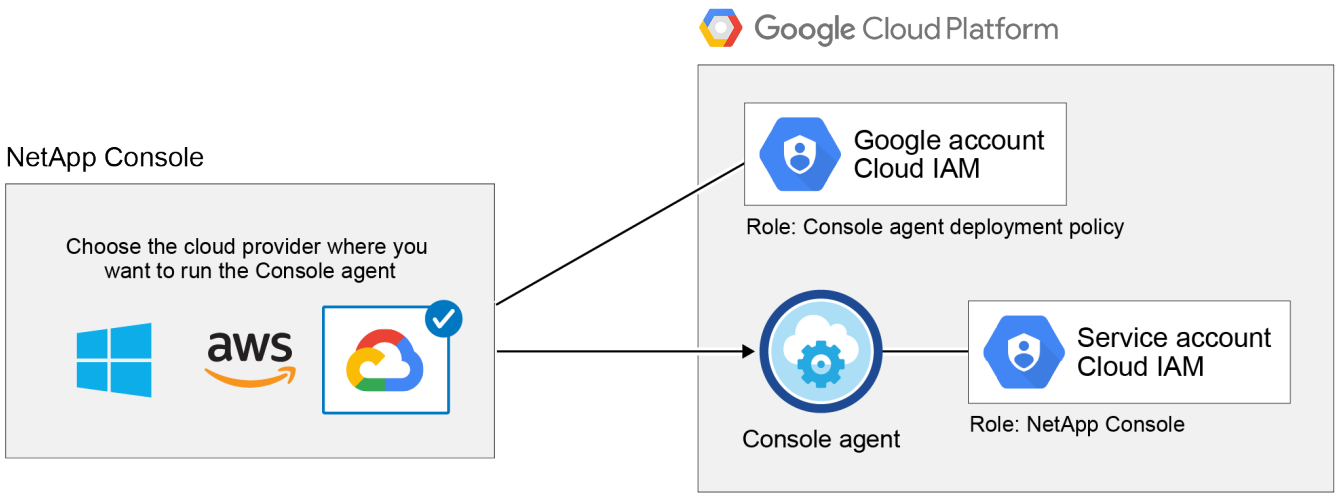
Proyecto y permisos para la NetApp Console

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"

Administra las credenciales y suscripciones de Google Cloud para NetApp Console

Puedes gestionar las credenciales de Google Cloud que están asociadas con una instancia de VM del agente de Console al asociar una suscripción de marketplace y al solucionar problemas del proceso de suscripción. Ambas tareas aseguran que puedas usar tu suscripción de marketplace para pagar servicios de datos.

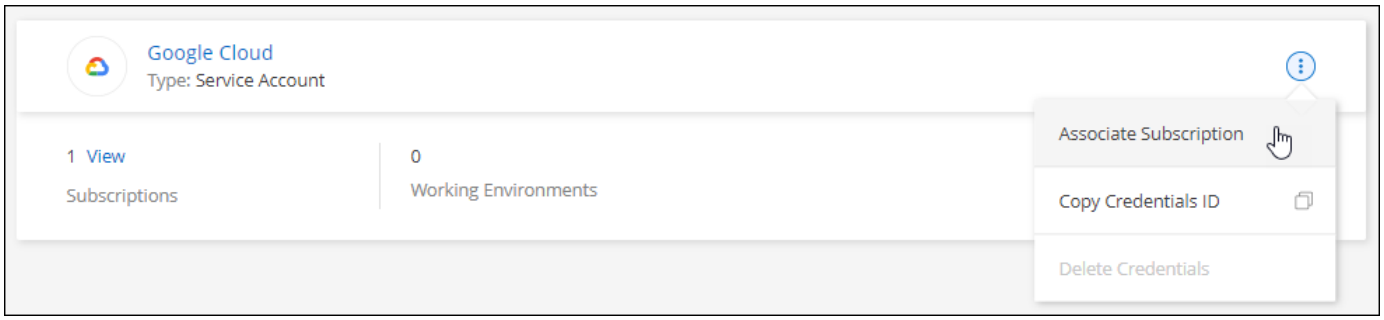
Asocia una suscripción de Marketplace con las credenciales de Google Cloud

Cuando implementas un agente de Console en Google Cloud, Console crea un conjunto predeterminado de credenciales que están asociadas con una instancia de VM del agente de Console. En cualquier momento, puedes cambiar la suscripción de Google Cloud Marketplace que está asociada con estas credenciales. La suscripción te permite crear un sistema Cloud Volumes ONTAP de pago por uso y usar otros servicios de datos.

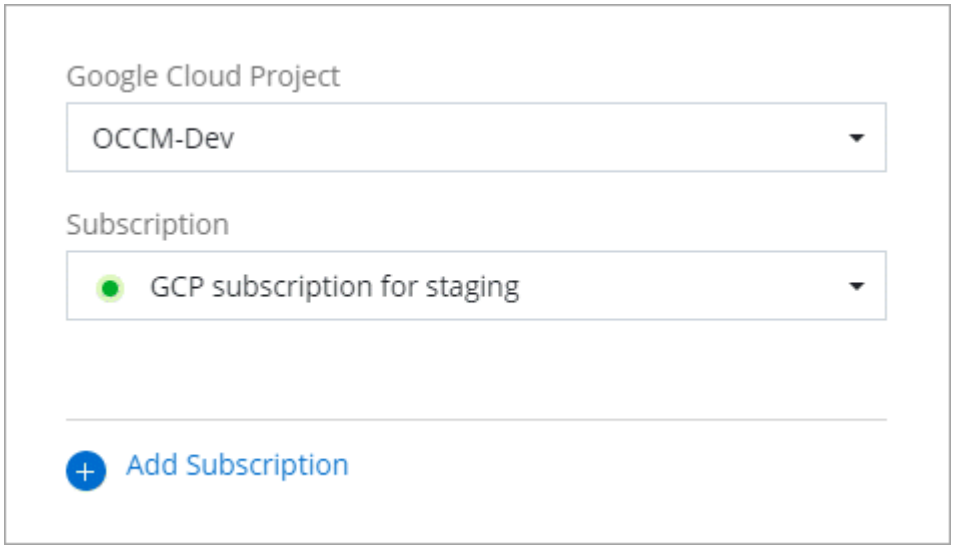
Reemplazar la suscripción actual del mercado por una nueva suscripción cambia la suscripción del mercado para cualquier sistema Cloud Volumes ONTAP existente y todos los sistemas nuevos.

Pasos

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



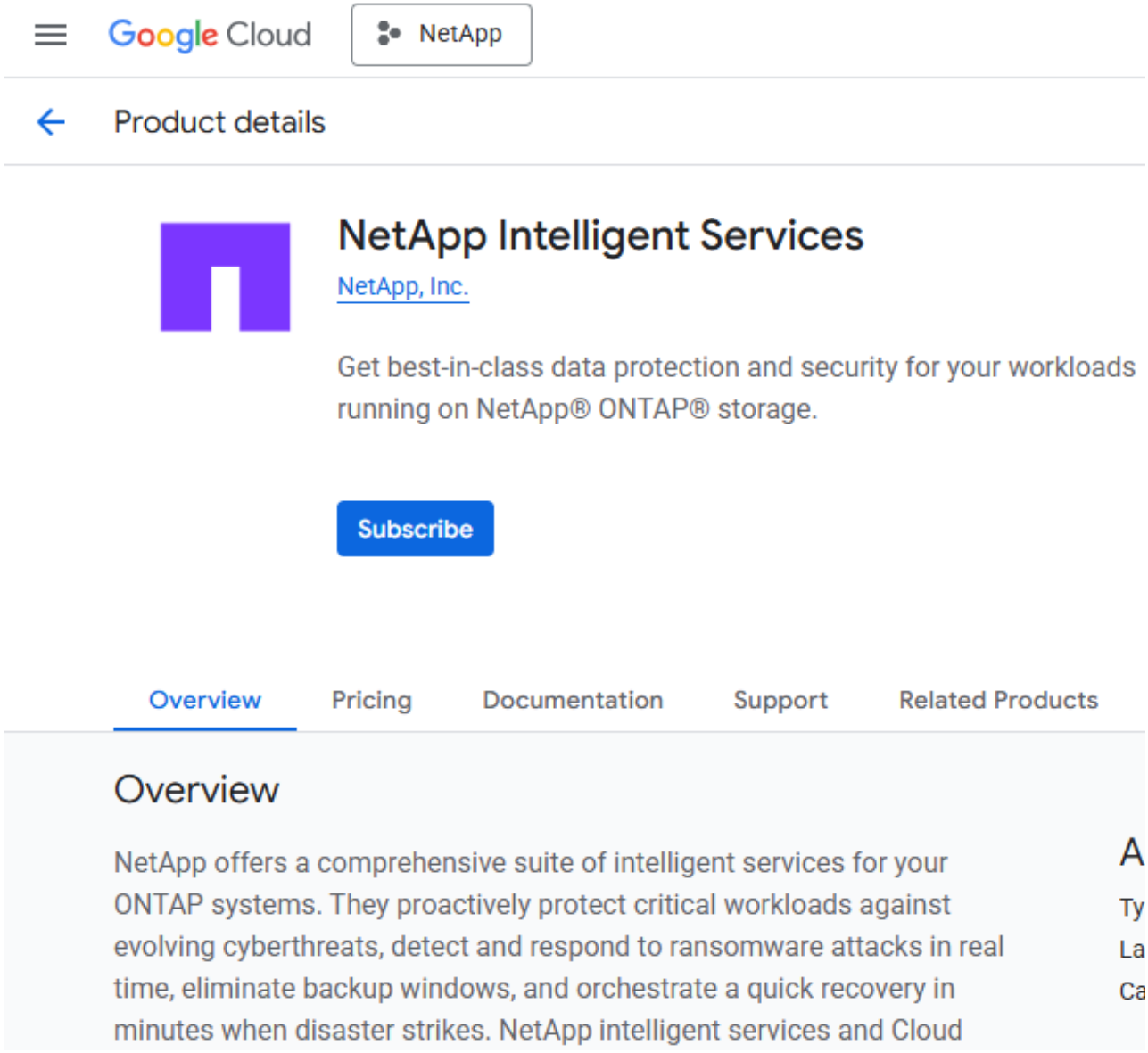
1. Para configurar una suscripción existente con las credenciales seleccionadas, seleccione un proyecto y una suscripción de Google Cloud de la lista desplegable y luego seleccione **Configurar**.



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

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

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

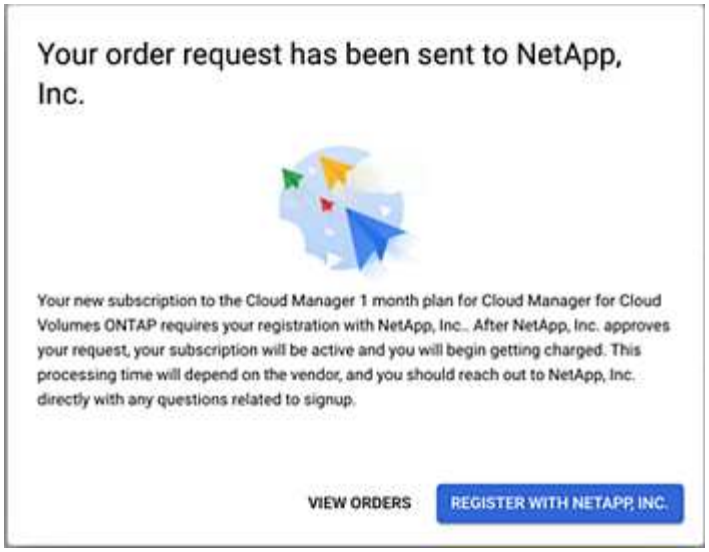


b. Seleccione **Suscribirse**.
c. Seleccione la cuenta de facturación adecuada y acepte los términos y condiciones.
d. Seleccione **Suscribirse**.

   Este paso envía su solicitud de transferencia a NetApp.

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

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



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

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

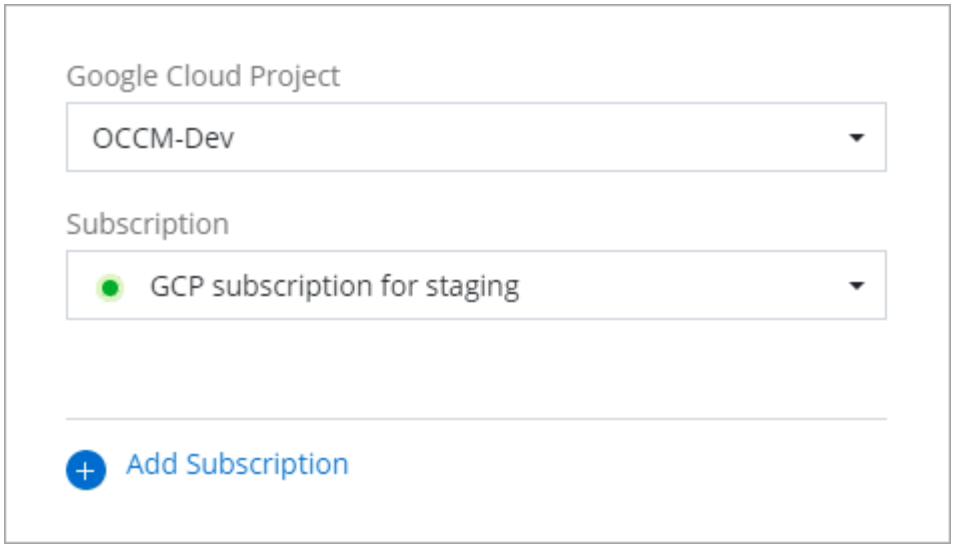
- Seleccione la organización de la consola con la que desea asociar esta suscripción.
- En el campo **Reemplazar suscripción existente**, elija si desea reemplazar automáticamente la suscripción existente de una organización con esta nueva suscripción.

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

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

- Seleccione **Guardar**.

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

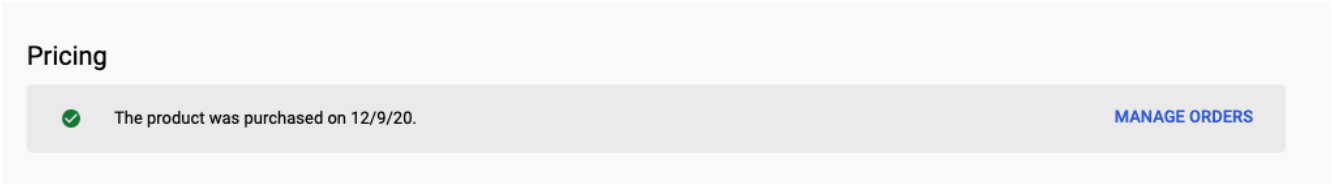


Soluciona problemas en el proceso de suscripción de Marketplace

A veces, suscribirse a los servicios de datos de NetApp a través de Google Cloud Marketplace puede volverse fragmentado por permisos incorrectos o por no seguir accidentalmente la redirección a la Consola. Si esto pasa, usa los siguientes pasos para completar el proceso de suscripción.

Pasos

1. Navega hasta "Página de NetApp en Google Cloud Marketplace" para comprobar el estado del pedido. Si la página indica **Manage on Provider**, desplázate hacia abajo y selecciona **Manage Orders**.



   - Si el pedido muestra una marca de verificación verde y esto es inesperado, es posible que otra persona de la organización que usa la misma cuenta de facturación ya esté suscrita. Si esto es inesperado o necesitas los detalles de esta suscripción, contacta a tu equipo de ventas de NetApp.

   - Si el pedido muestra un reloj y el estado **Pendiente**, vuelve a la página del marketplace y elige **Manage on Provider** para completar el proceso como se documentó arriba.

Gestión de identidad y acceso

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

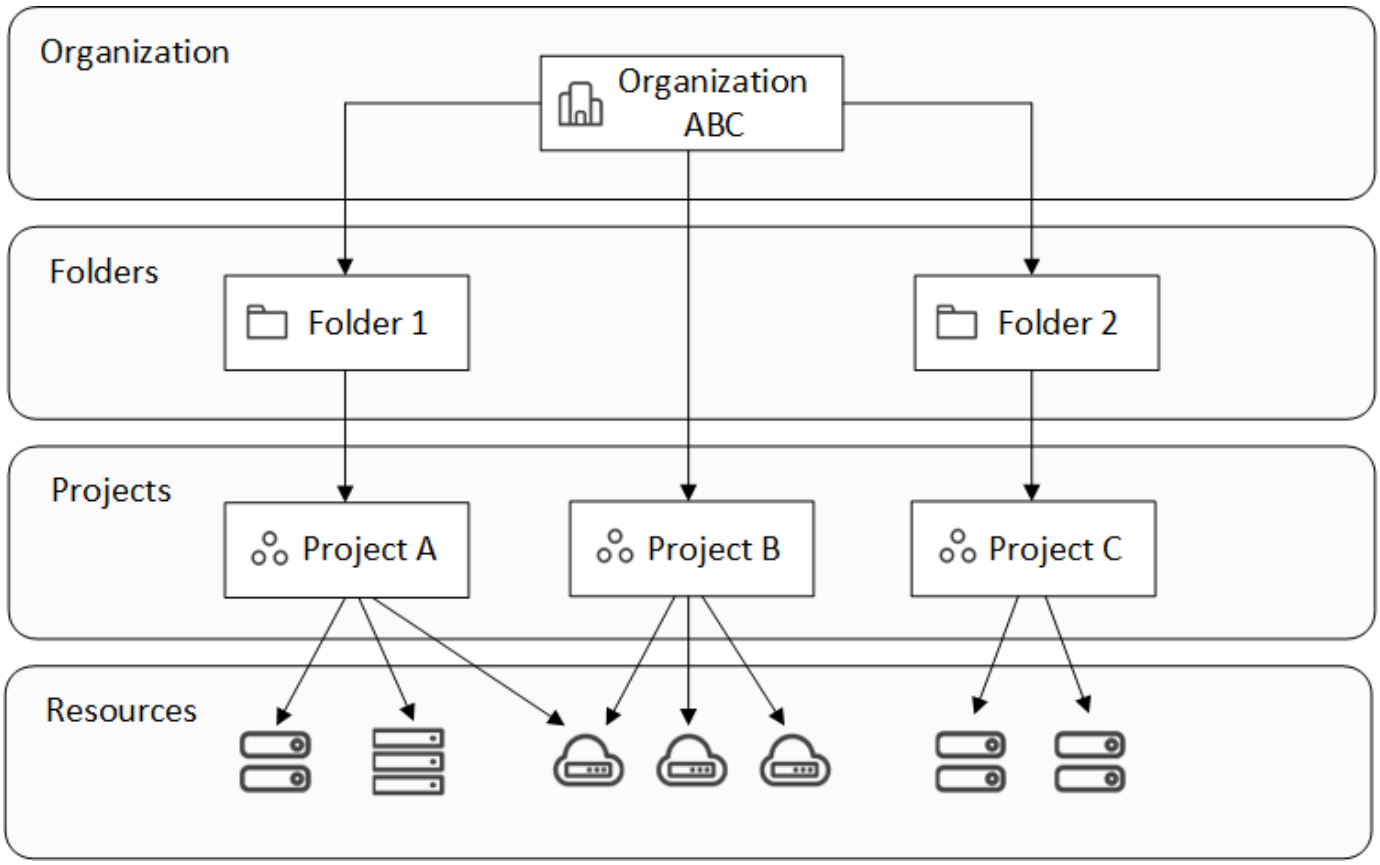
Utilice la gestión de identidad y acceso (IAM) de la consola de NetApp para organizar sus recursos de NetApp y controlar el acceso según la estructura de su negocio: por ubicación, departamento o proyecto.

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

Asigna roles de acceso a nivel de organización, carpeta o proyecto para que los usuarios tengan el acceso correcto a los recursos.

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

La siguiente imagen ilustra esta jerarquía en un nivel básico.



]

Componentes de gestión de identidad y acceso

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

Proyectos y carpetas dentro de su organización

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

Organización

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

Proyectos

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

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

"Aprenda cómo agregar proyectos a su organización."

Carpetas

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

"Aprenda cómo agregar carpetas a su organización."

Recursos

Un *recurso* es una entidad de la que la Console tiene conocimiento y que puede asignarse a un proyecto. *Recursos* incluyen sistemas de almacenamiento, suscripciones a Keystone, algunas cargas de trabajo de Backup and Recovery, así como agentes de la Console.

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

+

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

+

"Aprenda a asociar recursos a proyectos."

Sistemas de almacenamiento y suscripciones Keystone

Los sistemas de almacenamiento son los recursos principales que gestionas en NetApp Console. NetApp Console admite la gestión de sistemas de almacenamiento tanto locales como en la nube. Debes añadir un sistema de almacenamiento a un proyecto para que puedan acceder a él quienes estén asignados al proyecto.

Sistemas de almacenamiento

Los sistemas de almacenamiento se asocian automáticamente al proyecto donde se añaden, pero puedes asociarlos a otros proyectos o carpetas desde la página **Resources**. No puedes asociar sistemas de almacenamiento FSx para NetApp ONTAP a proyectos o carpetas, pero puedes verlos en la página

Systems o desde Workloads.

Suscripciones a Keystone

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

Cargas de trabajo de Backup and Recovery (Oracle y Microsoft SQL Server)

Algunas cargas de trabajo de Backup and Recovery también se consideran recursos. Puedes asignar permisos a los usuarios para acceder a Backup and Recovery

Agentes de consola

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

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

"Aprenda a asociar agentes con proyectos."

Miembros y roles

Miembros

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

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

"Aprenda cómo agregar miembros a su organización."

Roles de acceso

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

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

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

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

"Obtenga más información sobre los roles de acceso" .

Ejemplos de estrategias de IAM

Estrategia de organización pequeña

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

Ejemplo: Corporación ABC (equipo de 5 personas)

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

Estrategia empresarial multirregional

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

Ejemplo: Corporación XYZ (empresa multinacional)

- **Estructura:** Organización > Carpetas regionales (Norteamérica, Europa, Asia-Pacífico) > Carpetas de proyectos por región
- **Roles de plataforma:**
  - 1 **Administrador de la organización**: Supervisión global y gestión de políticas
  - 3 **Administradores de carpetas o proyectos**: Control regional (uno por región)
  - 1 **Administrador de la federación**: Integración del proveedor de identidad corporativa
- **Roles de almacenamiento por región:**
  - 9 **Administrador de almacenamiento**: descubre y administra sistemas de almacenamiento en regiones asignadas
  - 2 **Visor de almacenamiento**: Supervise los recursos de almacenamiento en todas las regiones
  - 1 **Especialista en salud del sistema**: Administra la salud del almacenamiento sin modificaciones del sistema
- **Roles de servicio de datos:**
  - **Administrador de copias de seguridad y recuperación**: por proyecto, según las responsabilidades de copia de seguridad
  - **Administrador de resiliencia ante ransomware**: Supervisión del equipo de seguridad en todos los proyectos
- **Estrategia del agente:** Agentes regionales asociados a proyectos geográficos apropiados
- **Beneficios:** Mayor seguridad mediante la segregación de roles, autonomía regional y cumplimiento de las regulaciones locales.

Estrategia de especialización departamental

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

Ejemplo: TechCorp (empresa tecnológica de tamaño mediano)

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

Próximos pasos con IAM en la NetApp Console

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

Comience a utilizar la identidad y el acceso en la NetApp Console

Cuando te registras en la NetApp Console, se te solicita que crees una nueva organización. La organización incluye un miembro (un administrador de la organización) y un proyecto predeterminado. Para configurar la gestión de identidad y acceso (IAM) para satisfacer las necesidades de su negocio, deberá personalizar la jerarquía de su organización, agregar miembros adicionales, agregar o descubrir recursos y asociar esos recursos en toda su jerarquía.

Necesita los permisos de **Administrador de la organización** o **Superadministrador** para administrar la identidad y el acceso de su organización. Con permisos de **Administrador de carpeta o proyecto**, puedes administrar solo las carpetas y los proyectos a los que tienes acceso.

Siga estos pasos para configurar una nueva organización. El orden puede variar según las necesidades de su organización.

1 Edite el proyecto predeterminado o agréguelo a la jerarquía de su organización

Utilice el proyecto predeterminado o cree proyectos y carpetas adicionales que coincidan con la jerarquía de su negocio.

"Aprenda a organizar sus recursos con carpetas y proyectos" .

2 Asociar miembros a su organización

Una vez que los usuarios se registren en NetApp Console, deberá agregarlos explícitamente a su organización de consola. También tiene la opción de agregar cuentas de servicio a su organización.

"Aprenda a administrar miembros y sus permisos" .

3 Agregar o descubrir recursos

Agregar o descubrir recursos (sistemas) a la consola. Los miembros de la organización gestionan los sistemas desde dentro de un proyecto.

Aprenda a crear o descubrir recursos:

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Sistemas de la serie E"
- "Clústeres ONTAP locales"
- "StorageGRID"

4 Asociar recursos con proyectos adicionales

Agregar o descubrir un sistema en la Consola asocia automáticamente el recurso con el proyecto seleccionado actualmente. Para que ese recurso esté disponible para otro proyecto de su organización, asócielo con el proyecto respectivo. Si se utiliza un agente de consola para administrar el recurso, asocie el agente de consola con el proyecto respectivo.

- "Aprenda a administrar la jerarquía de recursos de su organización" .
- "Aprenda a asociar un agente de consola con una carpeta o un proyecto" .

Información relacionada

- "Obtenga información sobre la gestión de identidad y acceso en la NetApp Console"
- "Conozca la API para identidad y acceso"

Configurar la organización de su consola

Agregue carpetas y proyectos a su organización de la NetApp Console

Agregue carpetas y proyectos para que coincidan con la estructura de su negocio. Después de crear carpetas y proyectos, puede asociar recursos a ellos y administrar el acceso de los miembros a esos proyectos.

La consola crea automáticamente un proyecto para usted cuando crea una nueva organización. La mayoría de las organizaciones necesitan más de un proyecto, así como carpetas para mantener las cosas organizadas. "Obtenga información sobre la jerarquía de recursos en la NetApp Console".

Uso de carpetas y proyectos para organizar recursos

En NetApp Console, una organización contiene carpetas y proyectos que lo ayudan a organizar sus recursos. Las carpetas le ayudan a agrupar proyectos relacionados, y los proyectos le ayudan a administrar los recursos y el acceso de los miembros.

Carpetas

Las carpetas le ayudan a organizar proyectos relacionados. Puede crear carpetas anidadas para representar diferentes niveles de la estructura de su organización. Por ejemplo, puede crear una carpeta de nivel superior para cada unidad de negocio y luego crear subcarpetas para diferentes equipos dentro de esa unidad de negocio. Luego crea proyectos dentro de carpetas.

Las carpetas también le permiten administrar el acceso de los miembros de manera más eficiente mediante la herencia de roles. Cuando se asignan roles a miembros a nivel de carpeta, estos heredan permisos para todos los proyectos y carpetas secundarios.

Las carpetas son una herramienta organizativa y no son visibles para los miembros que no tienen permisos de IAM, como el administrador de la organización, el administrador de la carpeta o del proyecto o los roles de superadministrador. Los miembros acceden a los proyectos, no a las carpetas.

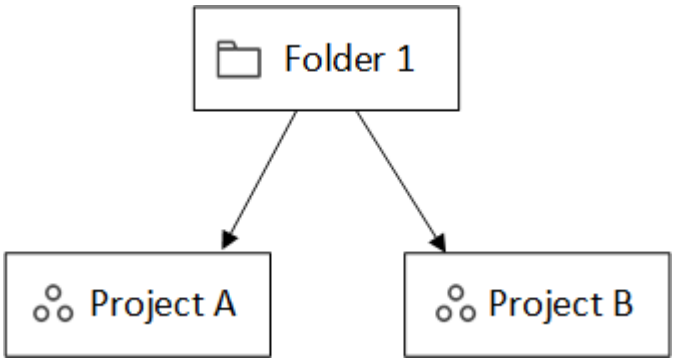
Los administradores de la organización pueden delegar responsabilidades administrativas mediante la creación de carpetas. Después de crear una carpeta, un administrador de la organización puede asignar a un miembro los roles de administrador de carpeta o proyecto para carpetas específicas. Estos miembros pueden luego administrar todos los proyectos dentro de esa carpeta sin tener acceso a toda la organización.

Las carpetas pueden tener otras carpetas o proyectos como hijos, pero no pueden tener recursos directamente asociados a ellas. Los recursos deben estar asociados a un proyecto.

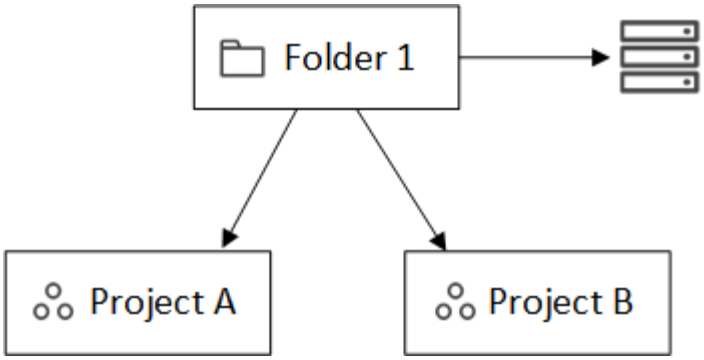
Cuándo asociar un recurso a una carpeta

Un *administrador de la organización* puede asociar un recurso con una carpeta para que un *administrador de carpeta o proyecto* pueda vincularlo a los proyectos apropiados en la carpeta.

Por ejemplo, digamos que tienes una carpeta que contiene dos proyectos:

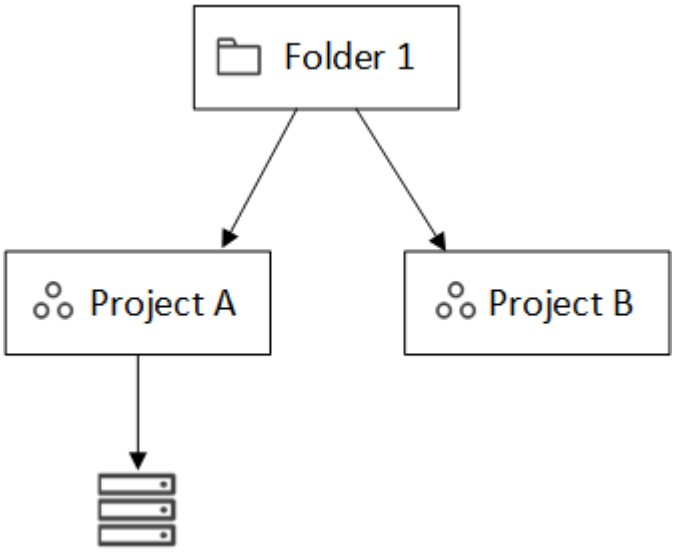


El *administrador de la organización* puede asociar un recurso con la carpeta:



Asociar un recurso a una carpeta no lo hace accesible a todos los proyectos; solo el administrador de la carpeta o del proyecto puede verlo. El administrador de carpeta o proyecto decide qué proyectos pueden acceder a él y asocia el recurso con los proyectos adecuados.

En este ejemplo, el administrador asocia el recurso con el Proyecto A:



Los miembros que tienen permisos para el proyecto A ahora pueden acceder al recurso.

Proyectos

Asociar recursos a proyectos para permitir que los miembros puedan administrarlos. Los recursos deben estar asociados a un proyecto para su administración y acceso por parte de los usuarios.

Una organización puede tener uno o varios proyectos. Un proyecto puede estar directamente bajo la organización o dentro de una carpeta. Si se utiliza un agente para descubrir recursos dentro de un proyecto, también debe asociar el agente con ese proyecto.

Los usuarios navegan entre los proyectos asignados en la página **Sistemas** para administrar los recursos asociados con cada proyecto.

Agregar una carpeta o proyecto

Agregue proyectos para administrar recursos y carpetas para agrupar proyectos relacionados. Cuando se crea una nueva organización, la Consola incluye un proyecto.

Puede crear hasta siete niveles de carpetas y proyectos en la estructura de recursos de su organización. Cree

carpetas anidadas para organizar sus recursos según sea necesario.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Organización**.
3. Desde la página **Organización**, seleccione **Agregar carpeta o proyecto**.
4. Seleccione **Carpeta** o **Proyecto**.
5. Introduzca los detalles de la carpeta o del proyecto:
   - **Nombre y ubicación**: Ingrese un nombre y elija una ubicación para la carpeta o el proyecto. Puede colocar carpetas o proyectos dentro de la organización o dentro de otra carpeta.
   - **Recursos**: Seleccione los recursos que desea asociar con esta carpeta o proyecto. Si aún no ha agregado sistemas de almacenamiento a la consola, puede realizar este paso más adelante.

     Los miembros no pueden acceder a los recursos de una carpeta hasta que esos recursos se asignen a un proyecto. Utilice carpetas para guardar recursos temporalmente hasta que cree los proyectos necesarios. Esto puede ayudar al administrador de la organización a delegar la asignación de recursos a un administrador de carpeta o proyecto, quien luego asigna recursos a los proyectos dentro de la carpeta.

   - **Acceso**: Seleccione **Agregar un miembro** para asignar acceso y un rol. Puede agregar o eliminar miembros del proyecto o carpeta en cualquier momento.

     "Obtenga más información sobre los roles de acceso" .
6. Seleccione **Agregar**.

Cambiar el nombre de una carpeta o proyecto

Cambie el nombre de una carpeta o proyecto según sea necesario. El cambio de nombre no afecta los recursos asociados ni el acceso de los miembros.

Pasos

1. Desde la página **Organización**, navegue hasta un proyecto o carpeta en la tabla, seleccione ••• y luego seleccione **Editar carpeta** o **Editar proyecto**.
2. En la página **Editar**, ingrese un nuevo nombre y seleccione **Aplicar**.

Eliminar una carpeta o proyecto

Elimina carpetas y proyectos que ya no necesites, por ejemplo, después de una reestructuración del equipo o de la finalización de un proyecto.

Antes de eliminar una carpeta o un proyecto, asegúrese de que no contenga ningún recurso. Aprenda a eliminar recursos.

Pasos

1. Desde la página **Organización**, navegue hasta un proyecto o carpeta en la tabla, seleccione ••• y luego seleccione **Eliminar**.
2. Confirme que desea eliminar la carpeta o el proyecto.

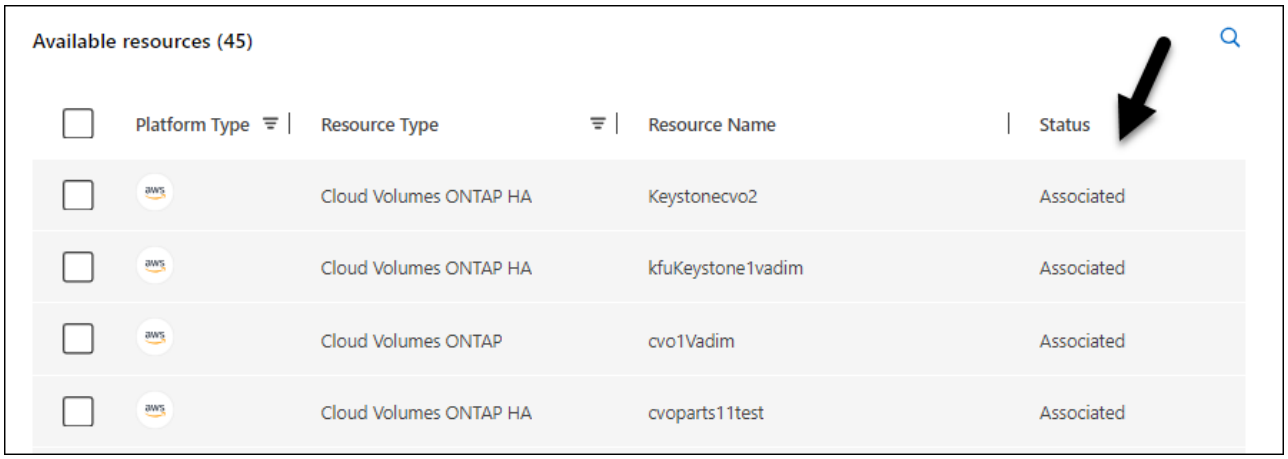
Ver los recursos asociados a una carpeta o proyecto

Ver qué recursos y miembros están asociados con una carpeta o proyecto.

Pasos

1. Desde la página **Organización**, navegue hasta un proyecto o carpeta en la tabla, seleccione ••• y luego seleccione **Editar carpeta** o **Editar proyecto**.

2. En la página **Editar**, puede ver detalles sobre la carpeta o el proyecto seleccionado expandiendo las secciones **Recursos** o **Acceso**.
   - Seleccione **Recursos** para ver los recursos asociados. En la tabla, la columna **Estado** identifica los recursos que están asociados con la carpeta o el proyecto.



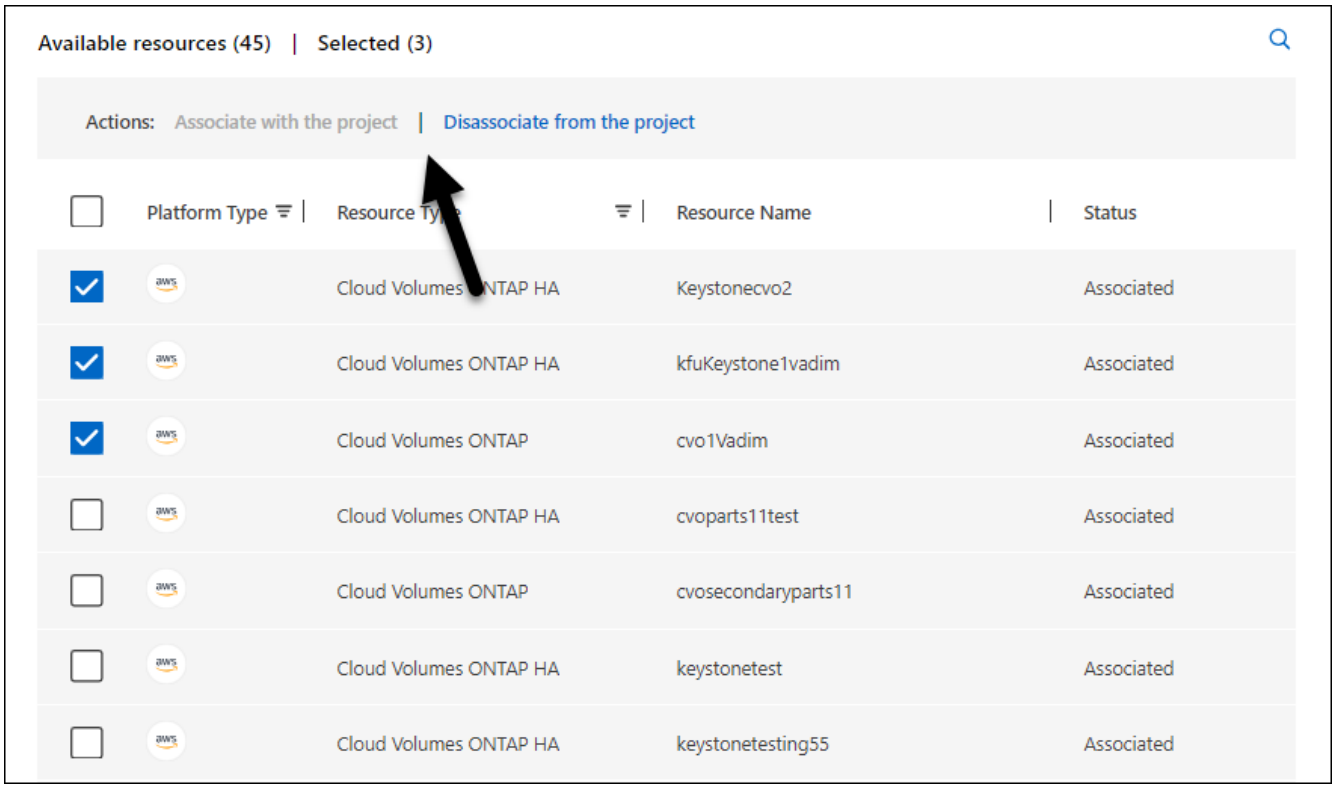
Cambiar los recursos asociados a una carpeta o proyecto

Puede cambiar los recursos asociados a una carpeta o proyecto a medida que cambian las necesidades de su organización.

Pasos

1. Desde la página **Organización**, navegue hasta un proyecto o carpeta en la tabla, seleccione ••• y luego seleccione **Editar carpeta** o **Editar proyecto**.
2. En la página **Editar**, seleccione **Recursos**.

   En la tabla, la columna **Estado** identifica los recursos que están asociados con la carpeta o el proyecto.
3. Seleccione los recursos que desea asociar o disociar.
4. Según los recursos que haya seleccionado, seleccione **Asociar con el proyecto** o **Desasociar del proyecto**.



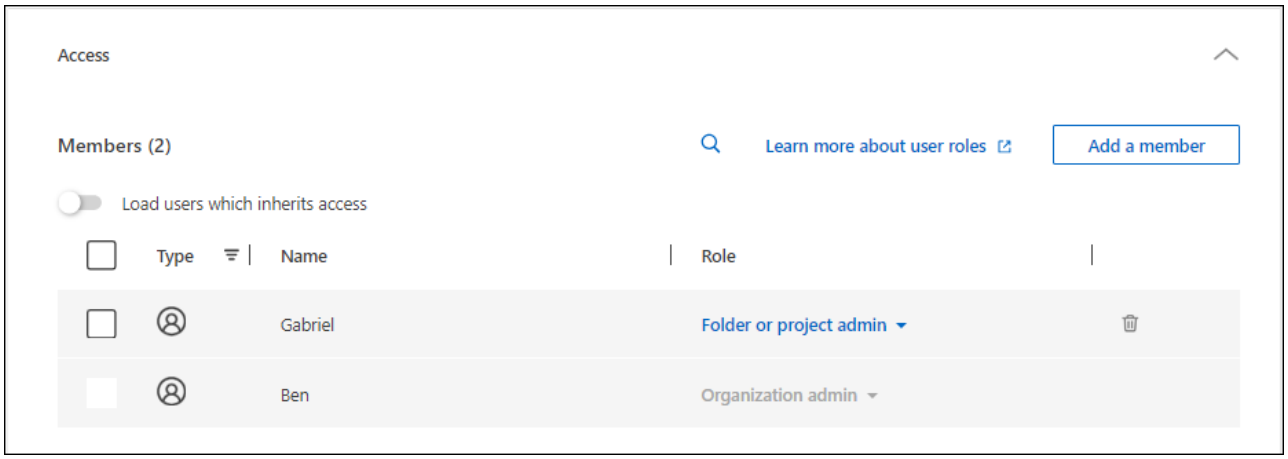
5. Seleccione **Aplicar**.

Ver miembros asociados a una carpeta o proyecto

Puede ver los miembros asociados a una carpeta o proyecto desde la página **Organización**.

Pasos

1. Desde la página **Organización**, navegue hasta un proyecto o carpeta en la tabla, seleccione ••• y luego seleccione **Editar carpeta** o **Editar proyecto**.
2. En la página **Editar**, seleccione **Acceso** para ver la lista de miembros que tienen acceso a la carpeta o proyecto seleccionado.
   - Seleccione **Acceso** para ver los miembros que tienen acceso a la carpeta o al proyecto.



Modificar el acceso de los miembros a una carpeta o proyecto

Modificar el acceso de los miembros para controlar el acceso a los recursos. Recuerde que los roles asignados a nivel de carpeta son heredados por todos los proyectos y carpetas secundarios.

No se puede cambiar el acceso de los miembros en niveles inferiores si se hereda del nivel de carpeta o de organización. Cambiar el permiso del miembro en el nivel de jerarquía superior para cambiar el acceso. Alternativamente, puede "Administrar permisos desde la página Miembros".

Pasos

1. Desde la página **Organización**, navegue hasta un proyecto o carpeta en la tabla, seleccione ••• y luego seleccione **Editar carpeta** o **Editar proyecto**.
2. En la página **Editar**, seleccione **Acceso** para ver la lista de miembros que tienen acceso a la carpeta o proyecto seleccionado.
3. Modificar el acceso de los miembros:
   - **Agregar un miembro**: seleccione el miembro que desea agregar a la carpeta o proyecto y asígnele un rol.
   - **Cambiar el rol de un miembro**: para cualquier miembro con un rol distinto de Administrador de la organización, seleccione su rol existente y luego elija un nuevo rol.
   - **Eliminar acceso de miembros**: para los miembros que tienen un rol definido en la carpeta o el proyecto que estás viendo, puedes eliminar su acceso.
4. Seleccione **Aplicar**.

Información relacionada

- "Obtenga información sobre la identidad y el acceso en la NetApp Console"
- "Comience con la identidad y el acceso"
- "Conozca la API de identidad y acceso"

Agregar recursos a carpetas y proyectos en la NetApp Console

Controle el acceso de los usuarios a los recursos agregándolos a proyectos y carpetas en su organización de la NetApp Console . Otorgar acceso a los usuarios a nivel de proyecto.

Un *recurso* es una entidad que la consola reconoce, como un recurso de almacenamiento, un agente de consola o una carga de trabajo de copia de seguridad y recuperación.

Puede ver y administrar recursos desde la página **Recursos** en la Consola.

Tipos de recursos de la consola

Puede asociar varios tipos de recursos a proyectos en su organización de NetApp Console :

Recursos de almacenamiento

Los recursos de almacenamiento son el tipo de recurso más común en su organización y representan sistemas de almacenamiento locales y en la nube. Cuando agrega un sistema de almacenamiento a la Consola, puede agregarlo a una carpeta o proyecto. Hasta entonces, la consola lo marca como no descubierto y no lo muestra en la página **Recursos**.

Agentes de consola

Si utilizó un agente de consola para descubrir sistemas de almacenamiento, agregue el agente a la misma carpeta o proyecto. Esto permite a los usuarios realizar funciones habilitadas por el agente, como servicios de datos o administración de almacenamiento nativo de la consola. Puede agregar agentes a carpetas o proyectos desde la página **Agentes** en la Consola. "Aprenda a asociar un agente de consola con una carpeta o un proyecto".

Suscripciones a Keystone

Si tiene suscripciones de Keystone en su organización, puede verlas en la página **Recursos**. Puede asociar suscripciones de Keystone con carpetas o proyectos para proporcionar acceso a los miembros que tienen permisos para esas carpetas o proyectos.

Ver los recursos de su organización

Puede ver los recursos descubiertos y no descubiertos asociados con su organización. El sistema encuentra recursos de almacenamiento y los marca como no descubiertos hasta que los agregue a la consola.

> La consola excluye los recursos de Amazon FSx for NetApp ONTAP de la página Recursos porque los usuarios no pueden asociarlos con un rol. Puede ver estos recursos en la página **Sistemas** o desde Cargas de trabajo.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Recursos**.
3. Seleccione **Búsqueda avanzada y filtrado**.
4. Utilice las opciones disponibles para encontrar un recurso:
   - **Buscar por nombre de recurso**: Ingrese una cadena de texto y seleccione **Agregar**.
   - **Plataforma**: seleccione una o más plataformas, como Amazon Web Services.
   - **Recursos**: seleccione uno o más recursos, como Cloud Volumes ONTAP.
   - **Organización, carpeta o proyecto**: seleccione toda la organización, una carpeta específica o un proyecto específico.
5. Seleccione **Buscar**.

Asociar un recurso con carpetas y proyectos

Asocie un recurso a una carpeta o proyecto para que esté disponible para los miembros que tengan permisos para esa carpeta o proyecto.

Pasos

1. Desde la página **Recursos**, navegue hasta un recurso en la tabla, seleccione ••• y luego seleccione **Asociar a carpetas o proyectos**.
2. Seleccione una carpeta o proyecto y luego seleccione **Aceptar**.
3. Para asociar una carpeta o proyecto adicional, seleccione **Agregar carpeta o proyecto** y luego seleccione la carpeta o el proyecto.

   Tenga en cuenta que solo puede seleccionar entre las carpetas y los proyectos para los que tiene permisos de administrador.

4. Seleccione **Recursos asociados**.
    - Si asoció el recurso con proyectos, los miembros que tienen permisos para esos proyectos ahora tienen la posibilidad de acceder al recurso desde la Consola.
    - Si asoció el recurso con una carpeta, un administrador de carpeta o proyecto ahora puede acceder al recurso y asociarlo con un proyecto dentro de la carpeta. "Obtenga información sobre cómo asociar un recurso con una carpeta".

Después de terminar

Si descubre un recurso mediante un agente de consola, asocie el agente de consola con el proyecto para otorgar acceso. De lo contrario, los miembros sin el rol de *Administrador de la organización* no podrán acceder al agente de la consola ni a su recurso asociado.

"Aprenda a asociar un agente de consola con una carpeta o un proyecto".

Ver las carpetas y proyectos asociados a un recurso

Puede ver las carpetas y proyectos asociados con un recurso en particular.

Si necesita saber qué miembros de la organización tienen acceso al recurso, puede"Ver los miembros que tienen acceso a las carpetas y proyectos asociados con el recurso" .

Pasos

1. Desde la página **Recursos**, navegue hasta un recurso en la tabla, seleccione••• y luego seleccione **Ver detalles**.

El siguiente ejemplo muestra un recurso asociado a un proyecto.

Para ver qué miembros de la organización tienen acceso al recurso,"Ver miembros con acceso a carpetas y proyectos asociados" .

Eliminar un recurso de una carpeta o proyecto

Para eliminar un recurso de una carpeta o proyecto, elimine su asociación. Esto evita que los miembros administren el recurso en esa carpeta o proyecto.

Para eliminar un recurso descubierto de toda la organización, vaya a la página **Sistemas** y elimine el sistema.

Pasos

1. Desde la página **Recursos**, navegue hasta un recurso en la tabla, seleccione••• y luego seleccione **Ver detalles**.

2. Para eliminar un recurso de una carpeta o proyecto, seleccione junto a la carpeta o proyecto.
3. Seleccione **Eliminar** para eliminar la asociación.

Información relacionada

- "Obtenga información sobre la identidad y el acceso en la NetApp Console"
- "Comience a utilizar la identidad y el acceso en la NetApp Console"
- "Conozca la API para identidad y acceso"

Asociar un agente de consola con otras carpetas y proyectos

Asocie agentes de la consola con proyectos específicos para habilitar la administración de recursos y el acceso al servicio de datos. Los recursos descubiertos a través de un agente de consola requieren que tanto el recurso como el agente estén asociados con los mismos proyectos respectivos para el acceso del equipo.

Los superadministradores y administradores de organizaciones pueden crear agentes y asociar cualquier agente con cualquier proyecto o carpeta. Los administradores de carpetas o proyectos solo pueden asociar agentes existentes con carpetas y proyectos para los que tengan permisos. "Obtenga más información sobre las acciones que un administrador de carpeta o proyecto puede completar".

Pasos

1. Seleccione **Administración > Identidad y acceso** > **Agentes**.
2. Desde la tabla, busque el agente de consola que desea asociar.

   Utilice la búsqueda sobre la tabla para encontrar un agente de consola específico o filtrar la tabla por jerarquía de recursos.

3. Para ver las carpetas y los proyectos vinculados al agente de la consola, seleccione y luego seleccione **Ver detalles**.

   La página muestra detalles sobre las carpetas y los proyectos asociados con el agente de la consola.

4. Seleccione **Asociar a carpeta o proyecto**.
5. Seleccione una carpeta o proyecto y luego seleccione **Aceptar**.
6. Para asociar el agente de consola con una carpeta o proyecto adicional, seleccione **Agregar una carpeta o proyecto** y luego seleccione la carpeta o el proyecto.
7. Seleccione **Agente asociado**.

Después de terminar

Asocie los recursos del agente de consola con las mismas carpetas y proyectos desde la página **Recursos**.

"Aprenda a asociar un recurso con carpetas y proyectos" .

Información relacionada

- "Obtenga más información sobre los agentes de la NetApp Console"
- "Obtenga más información sobre la gestión de identidad y acceso de la NetApp Console"
- "Comience con la identidad y el acceso"

- "Conozca la API para la gestión de identidad y acceso"

Agregue usuarios a su organización de la consola

Agregar usuarios a una organización de la NetApp Console

Dentro de la consola, usted otorga a los usuarios acceso a proyectos o carpetas según un rol de acceso. Un *rol de acceso* contiene un conjunto de permisos que permiten a un miembro (usuario o cuenta de servicio) realizar acciones específicas en el nivel asignado de la jerarquía de recursos.

Roles de acceso requeridos

Superadministrador, administrador de la organización o administrador de carpeta o proyecto (para carpetas y proyectos que administra). "Obtenga más información sobre los roles de acceso".

Comprenda cómo se otorga el acceso en la NetApp Console

La NetApp Console utiliza el control de acceso basado en roles (RBAC) para administrar los permisos. Asignar roles a los usuarios individualmente o a través de grupos federados. Cada rol define acciones permitidas para recursos específicos.

Tenga en cuenta lo siguiente sobre cómo conceder acceso en la NetApp Console:

- Todos los usuarios deben registrarse primero en la NetApp Console antes de poder obtener acceso a los recursos.
- Debe asignar explícitamente un rol a cada usuario en la Consola antes de que puedan acceder a los recursos, incluso si son miembros de un grupo federado al que se le ha asignado un rol.
- Puede agregar cuentas de servicio directamente desde la consola y asignarles roles.

Agregue miembros a su organización

La NetApp Console admite tres tipos de miembros: cuentas de usuario, cuentas de servicio y grupos federados.

Los usuarios deben registrarse en NetApp Console antes de poder agregarlos y asignarles un rol, incluso si están en un grupo federado. Cree cuentas de servicio directamente en la consola.

Todos los miembros deben tener al menos un rol asignado explícitamente para poder acceder a los recursos.

Al agregar un miembro, elija el nivel de recurso (organización, carpeta o proyecto) y asigne un rol o roles con los permisos necesarios.

Agregar un usuario

Los usuarios se registran en la NetApp Console, pero un administrador de organización, carpeta o proyecto debe agregarlos a una organización, carpeta o proyecto para que puedan acceder a los recursos.

Antes de empezar:

El usuario ya debe haberse registrado en la NetApp Console. Si aún no se han registrado, diríjalos a "Regístrese en la NetApp Console."

Si está agregando un usuario que forma parte de un grupo federado, asegúrese de que el usuario ya se haya registrado en la NetApp Console y se le haya asignado explícitamente un rol en la consola. NetApp recomienda asignar un rol de acceso mínimo, como Visor de la organización.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione **Agregar un miembro**.
4. Para **Tipo de miembro**, mantenga **Usuario** seleccionado.
5. Para **Correo electrónico del usuario**, ingrese la dirección de correo electrónico del usuario asociada con el inicio de sesión que creó.
6. Utilice la sección **Seleccionar una organización, carpeta o proyecto** para elegir el nivel de su jerarquía de recursos para el cual el miembro debe tener permisos.

   Tenga en cuenta lo siguiente:

   - Puede seleccionar sólo las carpetas y proyectos para los que tenga permisos.
   - Cuando selecciona una organización o carpeta, otorga al miembro permisos sobre todo su contenido.
   - Solo puedes asignar el rol de **Administrador de la organización** a nivel de organización.
7. **Seleccione una categoría** y luego seleccione un **Rol** que proporcione al miembro permisos para los recursos asociados con la organización, carpeta o proyecto que seleccionó.

   "Obtenga más información sobre los roles de acceso" .
8. Para dar acceso a más carpetas, proyectos o roles, seleccione **Agregar rol**, elija la carpeta, el proyecto o la categoría de rol y seleccione un rol.
9. Seleccione **Agregar**.

   La consola envía instrucciones por correo electrónico al usuario.

Agregar una cuenta de servicio

Las cuentas de servicio le permiten automatizar tareas y conectarse de forma segura con las API de la consola. Elija un ID de cliente y un secreto para configuraciones simples, o JWT (JSON Web Token) para una mayor seguridad en entornos automatizados o nativos de la nube. Seleccione el método que cumpla con sus requisitos de seguridad.

Antes de empezar:

Para la autenticación JWT, prepare su clave pública o certificado.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione **Agregar un miembro**.
4. Para **Tipo de miembro**, seleccione **Cuenta de servicio**.
5. Introduzca un nombre para la cuenta de servicio.

6. Para utilizar la autenticación JWT, seleccione **Usar autenticación JWT de clave privada** y cargue su clave RSA pública o certificado. Omitir si se utiliza el ID del cliente y el secreto.

   Su certificado X.509. Debe estar en formato PEM, CRT o CER.

   a. Configure notificaciones de vencimiento para su certificado. Elija entre siete días o 30 días. Las notificaciones de vencimiento se envían por correo electrónico y se muestran en la consola a los usuarios con el rol de superadministrador o administrador de la organización.

7. Utilice la sección **Seleccionar una organización, carpeta o proyecto** para elegir el nivel de su jerarquía de recursos para el cual el miembro debe tener permisos.

   Tenga en cuenta lo siguiente:

   - Sólo puedes seleccionar entre las carpetas y proyectos para los que tienes permisos.
   - Al seleccionar una organización o carpeta, se otorgan al miembro permisos sobre todo su contenido.
   - Solo puedes asignar el rol de **Administrador de la organización** a nivel de organización.

8. Seleccione una **Categoría** y luego seleccione un **Rol** que le otorgue al miembro permisos para los recursos en la organización, carpeta o proyecto que usted seleccionó.

   "Obtenga más información sobre los roles de acceso" .

9. Para dar acceso a más carpetas, proyectos o roles, seleccione **Agregar rol**, elija la carpeta, el proyecto o la categoría de rol y seleccione un rol.
10. Si no eligió utilizar la autenticación JWT, descargue o copie el ID del cliente y el secreto del cliente.

    La consola muestra el secreto del cliente solo una vez. Cópielo de forma segura; podrá volver a crearlo más tarde si lo pierde.

11. Si eligió la autenticación JWT, descargue o copie el ID del cliente y la audiencia JWT. La consola muestra esta información solo una vez y no permite recuperarla más tarde.
12. Seleccione **Cerrar**.

Agregue un grupo federado a su organización

Puede agregar un grupo federado de su proveedor de identidad (IdP) a su organización y asignarle uno o más roles. Los miembros del grupo federado heredan los roles que usted asigna al grupo en la Consola.

Antes de poder asignar un rol a un grupo federado, asegúrese de lo siguiente:

- Configure la federación entre su IdP y la consola. "Aprenda cómo configurar la federación."
- El grupo ya debe existir en su IdP y debe tener asignado acceso a la aplicación de la Consola.
- Los usuarios que pertenecen al grupo ya deben haberse registrado en la NetApp Console y se les debe asignar explícitamente un rol en la consola. NetApp recomienda asignar un rol de acceso mínimo, como Visor de la organización.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione **Agregar un miembro**.
4. Para **Tipo de miembro**, seleccione **Grupo federado**.

5. Seleccione la federación de la que es miembro el grupo
6. Para **Nombre del grupo**, ingrese el nombre exacto del grupo en su IdP.
7. Utilice la sección **Seleccionar una organización, carpeta o proyecto** para elegir el nivel de su jerarquía de recursos para el cual el miembro debe tener permisos.

   Tenga en cuenta lo siguiente:

   - Sólo puedes seleccionar entre las carpetas y proyectos para los que tienes permisos.
   - Al seleccionar una organización o carpeta, se otorgan al miembro permisos sobre todo su contenido.
   - Solo puedes asignar el rol de **Administrador de la organización** a nivel de organización.
8. Seleccione una **Categoría** y luego seleccione un **Rol** que le otorgue al miembro permisos para los recursos en la organización, carpeta o proyecto que usted seleccionó.

   "Obtenga más información sobre los roles de acceso" .
9. Para dar acceso a más carpetas, proyectos o roles, seleccione **Agregar rol**, elija la carpeta, el proyecto o la categoría de rol y seleccione un rol.

Información relacionada

- "Obtenga información sobre la gestión de identidad y acceso en la NetApp Console"
- "Comience con la identidad y el acceso"
- "Roles de acceso a la NetApp Console"
- "Conozca la API para identidad y acceso"

Gestionar el acceso y la seguridad de los usuarios

Obtenga más información sobre el control de acceso basado en roles (RBAC) de la NetApp Console

Administre el acceso de los usuarios a la NetApp Console con control de acceso basado en roles (RBAC), asignando roles predefinidos a nivel de organización, carpeta o proyecto. Cada rol otorga permisos específicos que definen qué acciones pueden realizar los usuarios dentro de su ámbito asignado.

NetApp diseña roles de consola con privilegios mínimos, por lo que cada rol incluye solo los permisos necesarios para sus tareas. Este enfoque mejora la seguridad al limitar el acceso a lo que cada miembro necesita.

Después de organizar los recursos en carpetas y proyectos, asigne a los miembros de la organización uno o más roles para carpetas o proyectos específicos, que les permitan realizar solo sus responsabilidades.

Por ejemplo, puede asignar a un miembro el rol de administrador de resiliencia ante ransomware para un nivel de proyecto específico, lo que le permitirá realizar operaciones de resiliencia ante ransomware para recursos dentro de ese proyecto, sin otorgarle un acceso más amplio a toda la organización. A este mismo usuario se le puede otorgar el rol para varios proyectos dentro de su organización.

Puede asignar a los usuarios múltiples roles para el mismo ámbito o para ámbitos diferentes, según sus responsabilidades. Por ejemplo, una organización más pequeña puede tener el mismo usuario que administre las tareas de Resiliencia ante Ransomware y Copia de Seguridad y Recuperación a nivel de la organización, mientras que una organización más grande puede tener diferentes usuarios asignados a cada rol a nivel de

proyecto.

Tipos de miembros de la organización de la consola

Hay tres tipos de miembros en una organización de la NetApp Console : * *Cuentas de usuario*: Usuarios individuales que inician sesión en la NetApp Console para administrar recursos. Los usuarios deben registrarse en la NetApp Console antes de poder agregarlos a una organización. * *Cuentas de servicio*: Cuentas no humanas utilizadas por aplicaciones o servicios para interactuar con la NetApp Console a través de API. Puede agregar cuentas de servicio directamente a su organización de la consola. * *Grupos federados*: Grupos sincronizados desde su proveedor de identidad (IdP) que le permiten administrar el acceso de múltiples usuarios de forma colectiva. Cada usuario dentro de un grupo federado debe haberse registrado en la NetApp Console y haber sido agregado a su organización con un rol de acceso antes de poder acceder a los recursos otorgados al grupo.

"Aprenda cómo agregar miembros a su organización."

Roles predefinidos en la NetApp Console

La NetApp Console incluye roles predefinidos que puedes asignar a los miembros de la organización. Cada rol incluye permisos que especifican qué acciones puede realizar un miembro dentro de su ámbito asignado (organización, carpeta o proyecto).

Los roles de la NetApp Console utilizan principios de privilegios mínimos que garantizan que los miembros solo tengan los permisos necesarios para sus tareas y categorizan los roles según el tipo de acceso que brindan:

- Roles de la plataforma: proporcionar permisos de administración de la consola
- Funciones de servicios de datos: proporcione permisos para administrar servicios de datos específicos, como Resiliencia ante ransomware y Copia de seguridad y recuperación
- Roles de la aplicación: Proporcionan permisos para administrar el almacenamiento, así como para auditar eventos y alertas de la consola.

Puede asignar múltiples roles a un miembro según sus responsabilidades. Por ejemplo, puede asignar a un miembro el rol de administrador de resiliencia contra ransomware y el rol de administrador de copia de seguridad y recuperación para un proyecto específico.

"Obtenga información sobre los roles predefinidos disponibles en NetApp Console".

Administrar el acceso de los miembros en la NetApp Console

Administrar el acceso de los miembros en su organización de la consola. Asignar roles para establecer permisos. Eliminar miembros cuando se van.

Roles de acceso requeridos

Superadministrador, administrador de la organización o administrador de carpeta o proyecto (para carpetas y proyectos que administra). Enlace:reference-iam-predefined-roles.html[Obtenga información sobre los roles de acceso].

Puede asignar roles de acceso por proyecto o carpeta. Por ejemplo, asigne un rol a un usuario para dos proyectos específicos o asigne el rol a nivel de carpeta para darle a un usuario el rol de administrador de Ransomware Resilience para todos los proyectos en una carpeta.

Agregue sus carpetas y proyectos antes de asignar acceso a los usuarios. "Aprenda a agregar carpetas y proyectos."

Comprenda cómo se otorga el acceso en la NetApp Console

La NetApp Console utiliza un modelo de control de acceso basado en roles (RBAC) para administrar los permisos de los usuarios. Puede asignar roles predefinidos a los miembros de forma individual o a través de grupos federados. Puede agregar y asignar roles a cuentas de servicio, así como a grupos federados. Cada rol define qué acciones puede realizar un miembro en los recursos asociados.

Tenga en cuenta lo siguiente sobre cómo conceder acceso en la NetApp Console:

- Todos los usuarios deben registrarse primero en la NetApp Console antes de poder obtener acceso a los recursos.
- Debe asignar explícitamente un rol a cada usuario en la Consola antes de que puedan acceder a los recursos, incluso si son miembros de un grupo federado al que se le ha asignado un rol.
- Puede agregar cuentas de servicio directamente desde la consola y asignarles roles.

Uso de la herencia de roles

Cuando se asigna un rol a nivel de organización, carpeta o proyecto en NetApp Console, ese rol es heredado automáticamente por todos los recursos dentro del alcance seleccionado. Por ejemplo, los roles a nivel de carpeta se aplican a todos los proyectos contenidos, mientras que los roles a nivel de proyecto se aplican a todos los recursos dentro de ese proyecto.

Ver miembros de la organización

Para comprender qué recursos y permisos están disponibles para un miembro, puede ver los roles asignados al miembro en diferentes niveles de la jerarquía de recursos de su organización."Aprenda a usar roles para controlar el acceso a los recursos de la consola."

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.

   La tabla **Miembros** enumera los miembros de su organización.

3. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Ver detalles**.

Ver los roles asignados a un miembro

Puede verificar qué roles tienen asignados actualmente.

Si tiene el rol de *Administrador de carpeta o de proyecto*, la página muestra todos los miembros de la organización. Sin embargo, solo puede ver y administrar los permisos de miembros para las carpetas y proyectos para los que tiene permisos. "Obtenga más información sobre las acciones que un administrador de carpeta o proyecto puede completar" .

1. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Ver detalles**.
2. En la tabla, expanda la fila correspondiente a la organización, carpeta o proyecto donde desea ver el rol

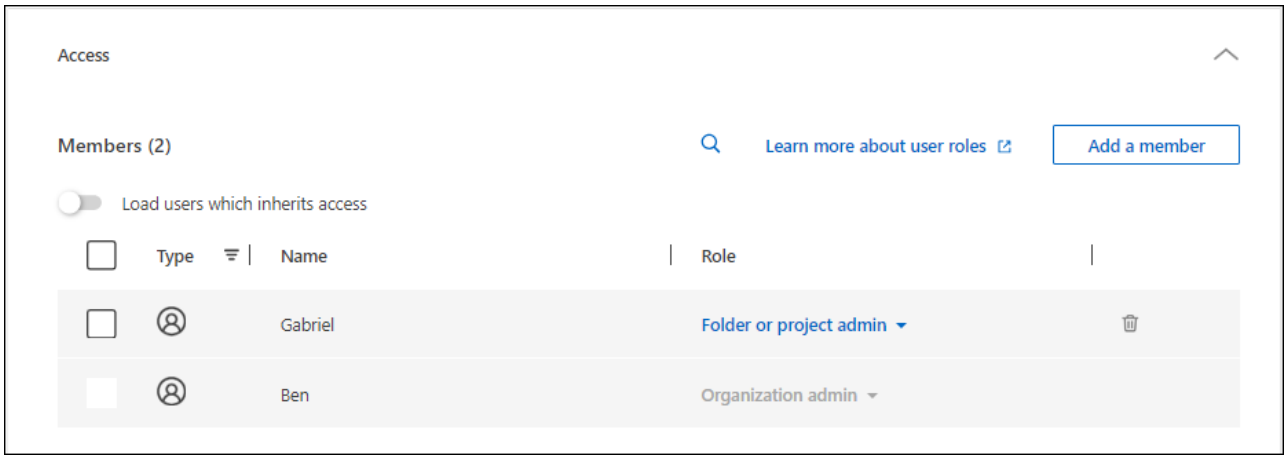
asignado al miembro y seleccione **Ver** en la columna **Rol**.

Ver miembros asociados a una carpeta o proyecto

Puede ver los miembros que tienen acceso a una carpeta o proyecto específico.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Organización**.
3. Desde la página **Organización**, navegue hasta un proyecto o carpeta en la tabla, seleccione ••• y luego seleccione **Editar carpeta** o **Editar proyecto**.
   - Seleccione **Acceso** para ver los miembros que tienen acceso a la carpeta o al proyecto.



Asignar o modificar el acceso de los miembros

Una vez que un usuario se registra en NetApp Console, puede agregarlo a su organización y asignarle un rol para brindarle acceso a los recursos. "Aprenda cómo agregar miembros a su organización."

Puede ajustar el acceso de un miembro agregando o eliminando roles según sea necesario.

Agregar un rol de acceso a un miembro

Normalmente, se asigna un rol al agregar un miembro a su organización, pero puede actualizarlo en cualquier momento eliminando o agregando roles.

Puede asignar a un usuario un rol de acceso para su organización, carpeta o proyecto.

Los miembros pueden tener múltiples roles dentro del mismo proyecto y en diferentes proyectos. Por ejemplo, las organizaciones más pequeñas pueden asignar todos los roles de acceso disponibles al mismo usuario, mientras que las organizaciones más grandes pueden hacer que los usuarios realicen tareas más especializadas. Como alternativa, también puede asignar a un usuario el rol de administrador de Resiliencia contra ransomware a nivel de la organización. En ese ejemplo, el usuario podría realizar tareas de resiliencia frente a ransomware en todos los proyectos dentro de su organización.

Su estrategia de roles de acceso debe estar alineada con la forma en que ha organizado sus recursos de NetApp .

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione una de las pestañas de miembros: **Usuarios**, **Cuentas de servicio** o **Grupos federados**.
4. Seleccione el menú de acciones ••• junto al miembro al que desea asignar un rol y seleccione **Agregar un rol**.
5. Para agregar un rol, complete los pasos en el cuadro de diálogo:
   - **Seleccione una organización, carpeta o proyecto**: elija el nivel de su jerarquía de recursos para el cual el miembro debe tener permisos.

     Si selecciona la organización o una carpeta, el miembro tendrá permisos sobre todo lo que resida dentro de la organización o carpeta.
   - **Seleccionar una categoría**: Elija una categoría de rol. "Obtenga más información sobre los roles de acceso" .
   - Seleccionar un **Rol**: elija un rol que proporcione al miembro permisos para los recursos asociados con la organización, carpeta o proyecto que seleccionó.
   - **Agregar rol**: si desea proporcionar acceso a carpetas o proyectos adicionales dentro de su organización, seleccione **Agregar rol**, especifique otra carpeta, proyecto o categoría de rol y luego seleccione una categoría de rol y un rol correspondiente.
6. Seleccione **Agregar nuevos roles**.

Cambiar el rol asignado a un miembro

Cambiar los roles de un miembro para actualizar su acceso.

> ⓘ Los usuarios deben tener al menos un rol asignado. No se pueden eliminar todos los roles de un usuario. Si necesita eliminar todos los roles, debe eliminar el usuario de su organización.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione una de las pestañas de miembros: **Usuarios**, **Cuentas de servicio** o **Grupos federados**.
4. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Ver detalles**.
5. En la tabla, expanda la fila correspondiente a la organización, carpeta o proyecto donde desea cambiar el rol asignado al miembro y seleccione **Ver** en la columna **Rol** para ver los roles asignados a este miembro.
6. Puede cambiar un rol existente de un miembro o eliminar un rol.
   a. Para cambiar el rol de un miembro, seleccione **Cambiar** junto al rol que desea cambiar. Sólo puedes cambiar un rol a un rol dentro de la misma categoría de rol. Por ejemplo, puede cambiar de un rol de servicio de datos a otro. Confirmar el cambio.
   b. Para desasignar el rol de un miembro, seleccione 🗑 junto al rol para eliminar el rol respectivo del miembro.. Se le pedirá que confirme la eliminación.

Eliminar un miembro de su organización

Eliminar a un miembro si abandona tu organización.

Cuando se elimina un miembro, el sistema revoca sus permisos de consola, pero conserva sus cuentas de consola y del sitio de soporte de NetApp .

Miembros federados

- Los usuarios federados pierden automáticamente el acceso a la NetApp Console cuando se los elimina de su IdP. Pero aún así debes eliminarlos de tu organización de consola para mantener tu lista de miembros actualizada.
- Si elimina un usuario de un grupo federado en su IdP, perderá el acceso a la consola asociado con ese grupo. Sin embargo, aún conservan cualquier acceso asociado con un rol explícito asignado a ellos en la Consola.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. Seleccione una de las pestañas de miembros: **Usuarios**, **Cuentas de servicio** o **Grupos federados**.
4. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• luego seleccione **Eliminar usuario**.
5. Confirme que desea eliminar al miembro de su organización.

Seguridad del usuario

Proteja el acceso de los usuarios a su organización de NetApp Console administrando la configuración de seguridad de los miembros. Puede restablecer las contraseñas de usuario, administrar la autenticación multifactor (MFA) y recrear las credenciales de la cuenta de servicio.

Roles de acceso requeridos

Superadministrador, administrador de la organización o administrador de carpeta o proyecto (para carpetas y proyectos que administra). Enlace:reference-iam-predefined-roles.html[Obtenga información sobre los roles de acceso].

Restablecer contraseñas de usuario (solo usuarios locales)

Los administradores de la organización no pueden restablecer las contraseñas de los usuarios locales. Sin embargo, pueden indicar a los usuarios que restablezcan sus propias contraseñas.

Indique a un usuario que restablezca su contraseña desde la página de inicio de sesión de la consola seleccionando **¿Olvidó su contraseña?**.

Esta opción no está disponible para los usuarios de una organización federada.

Administrar la autenticación multifactor (MFA) de un usuario

Si un usuario pierde el acceso a su dispositivo MFA, puede eliminar o deshabilitar su configuración MFA.

La autenticación multifactor solo está disponible para usuarios locales. Los usuarios federados no pueden habilitar MFA.

Los usuarios deben configurar MFA nuevamente cuando inicien sesión después de la eliminación. Si el

usuario pierde temporalmente el acceso a su dispositivo MFA, puede usar su código de recuperación guardado para iniciar sesión.

Si no tienen su código de recuperación, deshabilite temporalmente MFA para permitir el inicio de sesión. Cuando deshabilita MFA para un usuario, esta se deshabilita solo durante ocho horas y luego se vuelve a habilitar automáticamente. Al usuario se le permite un inicio de sesión durante ese tiempo sin MFA. Después de las ocho horas, el usuario deberá utilizar MFA para iniciar sesión.

> Para administrar la autenticación multifactor de un usuario, debe tener una dirección de correo electrónico en el mismo dominio que el usuario afectado.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.

   La tabla **Miembros** enumera los miembros de su organización.

3. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Administrar autenticación multifactor**.
4. Elija si desea eliminar o deshabilitar la configuración MFA del usuario.

Recrear las credenciales para una cuenta de servicio

Puede crear nuevas credenciales para un servicio si las pierde o necesita actualizarlas.

Al crear nuevas credenciales se eliminan las antiguas. No puedes utilizar las credenciales antiguas.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Miembros**.
3. En la tabla **Miembros**, navegue hasta una cuenta de servicio, seleccione ••• y luego seleccione **Recrear secretos**.
4. Seleccione **Recrear**.
5. Descargue o copie el ID del cliente y el secreto del cliente.

   La consola muestra el secreto del cliente solo una vez. Asegúrese de copiarlo o descargarlo y almacenarlo de forma segura.

Roles de acceso a la NetApp Console

Obtenga más información sobre los roles de acceso a la NetApp Console

La gestión de identidad y acceso (IAM) en la NetApp Console proporciona roles predefinidos que puede asignar a los miembros de su organización en diferentes niveles de su jerarquía de recursos. Antes de asignar estos roles, debe comprender los permisos que incluye cada rol. Los roles se dividen en las siguientes categorías: plataforma, aplicación y servicio de datos.

Roles de la plataforma

Los roles de plataforma otorgan permisos de administración de la NetApp Console , incluida la asignación de roles y la gestión de usuarios. La consola tiene varios roles de plataforma.

Rol de la plataforma	Responsabilidades
"Administrador de la organización"	Permite a un usuario acceso sin restricciones a todos los proyectos y carpetas dentro de una organización, agregar miembros a cualquier proyecto o carpeta, así como realizar cualquier tarea y utilizar cualquier servicio de datos que no tenga un rol explícito asociado. Los usuarios con este rol administran su organización creando carpetas y proyectos, asignando roles, agregando usuarios y administrando sistemas si tienen las credenciales adecuadas. Este es el único rol de acceso que puede crear agentes de consola.
"Administrador de carpetas o proyectos"	Permite a un usuario acceso sin restricciones a los proyectos y carpetas asignados. Pueden agregar miembros a las carpetas o proyectos que administran, así como realizar cualquier tarea y utilizar cualquier servicio de datos o aplicación en los recursos dentro de la carpeta o el proyecto que están asignados. Los administradores de carpetas o proyectos no pueden crear agentes de consola.
"Administración de la federación"	Permite a un usuario crear y administrar federaciones con la consola, lo que habilita el inicio de sesión único (SSO).
"Visor de la Federación"	Permite que un usuario vea las federaciones existentes con la consola. No se pueden crear ni administrar federaciones.
"Administración de asociaciones"	Permite a un usuario crear y gestionar asociaciones.
"Visor de asociaciones"	Permite a un usuario ver las asociaciones existentes. No se pueden crear ni gestionar asociaciones.
"Superadministrador"	Proporciona al usuario un subconjunto de roles de administrador. Esta función está diseñada para organizaciones más pequeñas que quizás no necesiten distribuir las responsabilidades de la consola entre varios usuarios.
"Súper espectador"	Proporciona al usuario un subconjunto de roles de espectador. Esta función está diseñada para organizaciones más pequeñas que quizás no necesiten distribuir las responsabilidades de la consola entre varios usuarios.

Roles de aplicación

La siguiente es una lista de roles en la categoría de aplicación. Cada rol otorga permisos específicos dentro de su alcance designado. Los usuarios que no tengan el rol de plataforma o aplicación requerido no pueden acceder a la aplicación respectiva.

Rol de la aplicación	Responsabilidades
"Administrador de Google Cloud NetApp Volumes"	Los usuarios con el rol de Google Cloud NetApp Volumes pueden descubrir y administrar Google Cloud NetApp Volumes.
"Visor de Google Cloud NetApp Volumes"	Los usuarios con el rol de usuario de Google Cloud NetApp Volumes pueden ver Google Cloud NetApp Volumes.

Rol de la aplicación	Responsabilidades
"Administrador de Keystone"	Los usuarios con el rol de administrador de Keystone pueden crear solicitudes de servicio. Permite a los usuarios supervisar y ver el uso, los recursos y los detalles de administración dentro del inquilino de Keystone al que están accediendo.
"Visor de Keystone"	Los usuarios con el rol de visualizador de Keystone NO PUEDEN crear solicitudes de servicio. Permite a los usuarios monitorear y visualizar el consumo, los activos y la información administrativa dentro del inquilino de Keystone al que están accediendo.
Rol de configuración del mediador de ONTAP	Las cuentas de servicio con la función de configuración de Mediador de ONTAP pueden crear solicitudes de servicio. Esta función es necesaria en una cuenta de servicio para configurar una instancia de la"Mediador de la nube de ONTAP" .
"Analista de soporte de operaciones"	Proporciona acceso a alertas y herramientas de monitoreo y la capacidad de ingresar y administrar casos de soporte.
"Administrador de almacenamiento"	Administrar las funciones de gobernanza y salud del almacenamiento, descubrir recursos de almacenamiento, así como modificar y eliminar sistemas existentes.
"Visor de almacenamiento"	Visualizar el estado del almacenamiento y las funciones de gobernanza, así como también los recursos de almacenamiento descubiertos previamente. No se pueden descubrir, modificar ni eliminar sistemas de almacenamiento existentes.
"Especialista en salud del sistema"	Administrar funciones de almacenamiento, salud y gobernanza, todos los permisos del administrador de almacenamiento, excepto no poder modificar ni eliminar sistemas existentes.

Roles de servicio de datos

La siguiente es una lista de roles en la categoría de servicio de datos. Cada rol otorga permisos específicos dentro de su alcance designado. Los usuarios que no tengan el rol de servicio de datos requerido o un rol de plataforma no podrán acceder al servicio de datos.

Rol de servicio de datos	Responsabilidades
"Superadministrador de copias de seguridad y recuperación"	Realice cualquier acción en NetApp Backup and Recovery.
"Administrador de copias de seguridad y recuperación"	Realice copias de seguridad en instantáneas locales, replique en almacenamiento secundario y realice copias de seguridad en almacenamiento de objetos.
"Administrador de restauración de copias de seguridad y recuperación"	Restaurar cargas de trabajo en Copia de seguridad y recuperación.
"Administrador de clones de Backup and Recovery"	Clonar aplicaciones y datos en Copia de seguridad y recuperación.
"Visor de copias de seguridad y recuperación"	Ver información de copia de seguridad y recuperación.

Rol de servicio de datos	Responsabilidades
"Administración de recuperación ante desastres"	Realice cualquier acción en el servicio NetApp Disaster Recovery .
"Administrador de conmutación por error de recuperación ante desastres"	Realizar conmutaciones por error y migraciones.
"Administrador de aplicaciones de recuperación ante desastres"	Cree planes de replicación, cámbielos e inicie conmutaciones por error de prueba.
"Visor de recuperación ante desastres"	Ver sólo información.
Visor de clasificación	Permite a los usuarios ver los resultados del análisis de NetApp Data Classification . Los usuarios con este rol pueden ver información de cumplimiento y generar informes para los recursos a los que tienen permiso de acceso. Estos usuarios no pueden habilitar ni deshabilitar el escaneo de volúmenes, depósitos o esquemas de bases de datos. La clasificación no tiene un rol de administrador.
"Administrador de resiliencia frente al ransomware"	Administre acciones en las pestañas Proteger, Alertas, Recuperar, Configuración e Informes de NetApp Ransomware Resilience.
"Visor de resiliencia contra ransomware"	Vea datos de carga de trabajo, vea datos de alerta, descargue datos de recuperación y descargue informes en Ransomware Resilience.
"Comportamiento del usuario de Resiliencia ante Ransomware"	Configure, administre y visualice la detección, alertas y monitoreo de comportamiento sospechoso de usuarios en Ransomware Resilience.
"Visor del comportamiento del usuario de Ransomware Resilience"	Vea alertas e información sobre comportamiento sospechoso de usuarios en Ransomware Resilience.
Administrador de SnapCenter	Proporciona la capacidad de realizar copias de seguridad de instantáneas de clústeres ONTAP locales mediante NetApp Backup and Recovery para aplicaciones. Un miembro que tiene este rol puede completar las siguientes acciones: * Completar cualquier acción desde Copia de seguridad y recuperación > Aplicaciones * Administrar todos los sistemas en los proyectos y carpetas para los que tiene permisos * Usar todos los servicios de la NetApp Console SnapCenter no tiene un rol de espectador.

Enlaces relacionados

- "Obtenga más información sobre la gestión de identidad y acceso de la NetApp Console"
- "Comience a utilizar NetApp Console IAM"
- "Administrar los miembros de la NetApp Console y sus permisos"
- "Obtenga más información sobre la API para NetApp Console IAM"

Roles de acceso a la plataforma de la NetApp Console

Asigne roles de plataforma a los usuarios para otorgar permisos para administrar la NetApp Console, asignar roles, agregar usuarios, crear agentes de consola y administrar

federaciones.

Ejemplo de roles organizacionales para una gran organización multinacional

XYZ Corporation organiza el acceso al almacenamiento de datos por región (América del Norte, Europa y Asia-Pacífico), proporcionando control regional con supervisión centralizada.

El **administrador de la organización** en la consola de XYZ Corporation crea una organización inicial y carpetas separadas para cada región. El administrador de carpeta o proyecto de cada región organiza los proyectos (con los recursos asociados) dentro de la carpeta de la región.

Los administradores regionales con el rol de **Administrador de carpeta o proyecto** administran activamente sus carpetas agregando recursos y usuarios. Estos administradores regionales también pueden agregar, eliminar o cambiar el nombre de las carpetas y los proyectos que administran. El **administrador de la organización** hereda los permisos para cualquier recurso nuevo, lo que mantiene la visibilidad del uso del almacenamiento en toda la organización.

Dentro de la misma organización, a un usuario se le asigna el rol de **administrador de federación** para administrar la federación de la organización con su IdP corporativo. Este usuario puede agregar o eliminar organizaciones federadas, pero no puede administrar usuarios ni recursos dentro de la organización. El **Administrador de la organización** asigna a un usuario el rol de **Visor de la federación** para verificar el estado de la federación y ver las organizaciones federadas.

Las siguientes tablas indican las acciones que cada rol de la plataforma de consola puede realizar.

Roles de administración de la organización

Tarea	Administrador de la organización	Administrador de carpetas o proyectos
Crear agentes	Sí	No
Crear, modificar o eliminar sistemas desde la consola (agregar o descubrir sistemas)	Sí	Sí
Crear carpetas y proyectos, incluida la eliminación	Sí	No
Cambiar el nombre de carpetas y proyectos existentes	Sí	Sí
Asignar roles y agregar usuarios	Sí	Sí
Asociar recursos con carpetas y proyectos	Sí	Sí
Asociar agentes con carpetas y proyectos	Sí	No
Eliminar agentes de carpetas y proyectos	Sí	No
Administrar agentes (editar certificados, configuraciones, etc.)	Sí	No
Administrar credenciales desde Administración > Credenciales	Sí	Sí
Crear, administrar y visualizar federaciones	Sí	No
Regístrese para recibir soporte y enviar casos a través de la Consola	Sí	Sí

Tarea	Administrador de la organización	Administrador de carpetas o proyectos
Utilice servicios de datos que no estén asociados a un rol de acceso explícito	Sí	Sí
Ver la página de Auditoría y notificaciones	Sí	Sí

Roles de la federación

Tarea	Administración de la federación	Visor de la Federación
Crear una federación	Sí	No
Verificar un dominio	Sí	No
Agregar un dominio a una federación	Sí	No
Deshabilitar y eliminar federaciones	Sí	No
Federaciones de pruebas	Sí	No
Ver federaciones y sus detalles	Sí	Sí

Roles de asociación

Tarea	Administración de asociaciones	Visor de asociaciones
Puede crear una asociación	Sí	No
Asignar roles a los miembros del socio	Sí	No
Puede agregar miembros a una asociación	Sí	No
Puede ver los detalles de la asociación de la organización	Sí	Sí

Roles de superadministrador y espectador

El rol de **Superadministrador** proporciona acceso completo para administrar las funciones de la consola, el almacenamiento y los servicios de datos. Este rol es adecuado para aquellos que supervisan la administración y la gobernanza. Por el contrario, el rol de **Supervisor** ofrece acceso de solo lectura, ideal para auditores o partes interesadas que necesitan visibilidad sin realizar cambios.

Las organizaciones deben utilizar el acceso de **superadministrador** con moderación para minimizar los riesgos de seguridad y alinearse con el principio del mínimo privilegio. La mayoría de las organizaciones deberían asignar roles específicos con solo los permisos necesarios para reducir el riesgo y mejorar la auditabilidad.

Ejemplo de roles super

ABC Corporation tiene un pequeño equipo de cinco personas que aprovecha la NetApp Console para los servicios de datos y la gestión del almacenamiento. En lugar de distribuir múltiples roles, asignan el rol de **Superadministrador** a dos miembros senior del equipo que manejan todas las tareas administrativas, incluida la gestión de usuarios y la configuración de recursos. A los tres miembros restantes del equipo se les asigna el rol de **Supervisor**, lo que les permite supervisar el estado del almacenamiento y el servicio de datos sin la posibilidad de modificar las configuraciones.

Role	Roles heredados
Superadministrador	• Administrador de la organización • Administrador de carpetas o proyectos • Administración de la federación • Administración de asociaciones • Administrador de resiliencia frente al ransomware • Administración de recuperación ante desastres • Superadministrador de respaldo • Administrador de almacenamiento • Administrador de Keystone • Administrador de Google Cloud NetApp Volumes
Súper espectador	• Visor de la organización • Visor de la Federación • Visor de asociaciones • Visor de resiliencia contra ransomware • Visor de recuperación ante desastres • Visor de copias de seguridad • Visor de almacenamiento • Visor de Keystone • Visor de Google Cloud NetApp Volumes

Roles de aplicación

Funciones de Google Cloud NetApp Volumes en la NetApp Console

Puede asignar la siguiente función a los usuarios para brindarles acceso a Google Cloud NetApp Volumes en la NetApp Console.

Google Cloud NetApp Volumes utiliza la siguiente función:

- * Administrador de Google Cloud NetApp Volumes *: descubre y administra Google Cloud NetApp Volumes en la consola.

- *Visor de Google Cloud NetApp Volumes *: Vea los Google Cloud NetApp Volumes en la consola.

Roles de acceso de Keystone en la NetApp Console

Los roles de Keystone brindan acceso a los paneles de Keystone y permiten a los usuarios ver y administrar su suscripción de Keystone . Hay dos roles de Keystone : administrador de Keystone y visor de Keystone . La principal diferencia entre los dos roles son las acciones que pueden realizar en Keystone. El rol de administrador de Keystone es el único rol que puede crear solicitudes de servicio o modificar suscripciones.

Ejemplo de roles de Keystone en la NetApp Console

XYZ Corporation tiene cuatro ingenieros de almacenamiento de diferentes departamentos que visualizan la información de suscripción de Keystone . Aunque todos estos usuarios necesitan supervisar la suscripción de Keystone , solo el líder del equipo puede realizar solicitudes de servicio. A tres de los miembros del equipo se les asigna el rol de *visualizador de Keystone *, mientras que al líder del equipo se le asigna el rol de *administrador de Keystone * para que haya un punto de control sobre las solicitudes de servicio de la empresa.

La siguiente tabla indica las acciones que puede realizar cada rol de Keystone .

Característica y acción	Administrador de Keystone	Visor de Keystone
Ver las siguientes pestañas: Suscripción, Activos, Monitor y Administración	Sí	Sí
*Página de suscripción de Keystone *:		
Ver suscripciones	Sí	Sí
Modificar o renovar suscripciones	Sí	No
*Página de activos de Keystone *:		
Ver activos	Sí	Sí
Administrar activos	Sí	No
*Página de alertas de Keystone *:		
Ver alertas	Sí	Sí
Administrar alertas	Sí	No
Crear alertas para mí mismo	Sí	Sí
* Licenses and subscriptions*:		
Puede ver licencias y suscripciones	Sí	Sí
*Página de informes de Keystone *:		

Característica y acción	Administrador de Keystone	Visor de Keystone
Descargar informes	Sí	Sí
Administrar informes	Sí	Sí
Crear informes para uno mismo	Sí	Sí
Solicitudes de servicio:		
Crear solicitudes de servicio	Sí	No
Ver solicitudes de servicio creadas por cualquier usuario dentro de la Organización	Sí	Sí

Rol de acceso de analista de soporte operativo para la NetApp Console

Puede asignar el rol de analista de soporte operativo a los usuarios para brindarles acceso a alertas y monitoreo. Los usuarios con este rol también pueden abrir casos de soporte.

Analista de soporte operativo

Tarea	Puede realizar
Administre sus propias credenciales de usuario desde Configuración > Credenciales	Sí
Ver recursos descubiertos	Sí
Regístrese para recibir soporte y enviar casos a través de la Consola	Sí
Ver la página de Auditoría y notificaciones	Sí
Ver, descargar y configurar alertas	Sí

Roles de acceso al almacenamiento para la NetApp Console

Puede asignar los siguientes roles a los usuarios para brindarles acceso a las funciones de administración de almacenamiento en la NetApp Console. Puede asignar a los usuarios un rol administrativo para administrar el almacenamiento o un rol de espectador para monitorear.

Estos roles no están disponibles desde la API de asociación de la NetApp Console .

Los administradores pueden asignar roles de almacenamiento a los usuarios para los siguientes recursos y funciones de almacenamiento:

Recursos de almacenamiento:

- Clústeres ONTAP locales
- StorageGRID
- Serie E

Servicios y características de la consola:

- Asesor digital
- Actualizaciones de software
- Planificación del ciclo de vida
- Sostenibilidad

Ejemplo de roles de almacenamiento en la NetApp Console

XYZ Corporation, una empresa multinacional, tiene un gran equipo de ingenieros de almacenamiento y administradores de almacenamiento. Permiten que este equipo administre los activos de almacenamiento de sus regiones y al mismo tiempo limite el acceso a las tareas principales de la consola, como la administración de usuarios, la creación de agentes y la administración de licencias.

Dentro de un equipo de 12 personas, a dos usuarios se les asigna el rol de **Visor de almacenamiento**, que les permite supervisar los recursos de almacenamiento asociados con los proyectos de consola a los que están asignados. A los nueve restantes se les asigna el rol de **administrador de almacenamiento**, que incluye la capacidad de administrar actualizaciones de software, acceder a ONTAP System Manager a través de la consola y también descubrir recursos de almacenamiento (agregar sistemas). A una persona del equipo se le asigna el rol de **Especialista en salud del sistema** para que pueda administrar la salud de los recursos de almacenamiento en su región, pero no modificar ni eliminar ningún sistema. Esta persona también puede realizar actualizaciones de software en los recursos de almacenamiento para los proyectos que se le asignan.

La organización tiene dos usuarios adicionales con el rol de **Administrador de la organización** que pueden administrar todos los aspectos de la Consola, incluida la administración de usuarios, la creación de agentes y la administración de licencias, así como varios usuarios con el rol de **Administrador de carpeta o proyecto** que pueden realizar tareas de administración de la Consola para las carpetas y los proyectos a los que están asignados.

La siguiente tabla muestra las acciones que realiza cada rol de almacenamiento.

Característica y acción	Administrador de almacenamiento	Especialista en salud del sistema	Visor de almacenamiento
Gestión de almacenamiento:			
Descubrir nuevos recursos (crear sistemas)	Sí	Sí	No
Ver sistemas descubiertos	Sí	Sí	No
Eliminar sistemas de la consola	Sí	No	No
Modificar sistemas	Sí	No	No
Crear agentes	No	No	No
Asesor digital			

Característica y acción	Administrador de almacenamiento	Especialista en salud del sistema	Visor de almacenamiento
Ver todas las páginas y funciones	Sí	Sí	Sí
* Licenses and subscriptions*			
Ver todas las páginas y funciones	No	No	No
Actualizaciones de software			
Ver página de destino y recomendaciones	Sí	Sí	Sí
Revise las posibles recomendaciones de versiones y los beneficios clave	Sí	Sí	Sí
Ver detalles de actualización de un clúster	Sí	Sí	Sí
Ejecute comprobaciones previas a la actualización y descargue el plan de actualización	Sí	Sí	Sí
Instalar actualizaciones de software	Sí	Sí	No
Planificación del ciclo de vida			
Revisar el estado de la planificación de la capacidad	Sí	Sí	Sí
Elija la siguiente acción (mejor práctica, nivel)	Sí	No	No
Almacene datos fríos en la nube y libere espacio	Sí	Sí	No
Configurar recordatorios	Sí	Sí	Sí
Sostenibilidad			
Ver el panel de control y las recomendaciones	Sí	Sí	Sí
Descargar datos del informe	Sí	Sí	Sí
Editar el porcentaje de mitigación de carbono	Sí	Sí	No
Recomendaciones de corrección	Sí	Sí	No
Aplazar recomendaciones	Sí	Sí	No
Acceso de administrador del sistema			
Puede ingresar credenciales	Sí	Sí	No

Característica y acción	Administrador de almacenamiento	Especialista en salud del sistema	Visor de almacenamiento
Cartas credenciales			
Credenciales de usuario	Sí	Sí	No

Roles de servicios de datos

Funciones de NetApp Backup and Recovery en la NetApp Console

Puede asignar los siguientes roles a los usuarios para brindarles acceso a NetApp Backup and Recovery dentro de la consola. Los roles de respaldo y recuperación le brindan la flexibilidad de asignar a los usuarios un rol específico para las tareas que necesitan realizar dentro de su organización. La forma de asignar roles depende de su propio negocio y de sus prácticas de gestión de almacenamiento.

El servicio utiliza los siguientes roles que son específicos de NetApp Backup and Recovery.

- **Superadministrador de Backup and Recovery**: realiza cualquier acción en NetApp Backup and Recovery.
- **Administrador de copias de seguridad y recuperación**: realice copias de seguridad en instantáneas locales, replique en almacenamiento secundario y realice copias de seguridad en acciones de almacenamiento de objetos en NetApp Backup and Recovery.
- **Administrador de restauración de copias de seguridad y recuperación**: restaure cargas de trabajo mediante NetApp Backup and Recovery.
- **Administrador de clones de respaldo y recuperación**: clona aplicaciones y datos usando NetApp Backup and Recovery.
- **Visor de copias de seguridad y recuperación**: ve información en NetApp Backup and Recovery, pero no realiza ninguna acción.

Para obtener detalles sobre todos los roles de acceso a la NetApp Console , consulte "La documentación de configuración y administración de la consola" .

Roles utilizados para acciones comunes

La siguiente tabla indica las acciones que cada rol de NetApp Backup and Recovery puede realizar para todas las cargas de trabajo.

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Administrador de clones de Backup and Recovery	Visor de copias de seguridad y recuperación
Agregar, editar o eliminar hosts	Sí	No	No	No	No
Instalar complementos	Sí	No	No	No	No

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Administrador de clones de Backup and Recovery	Visor de copias de seguridad y recuperación
Agregar credenciales (host, instancia, vCenter)	Sí	No	No	No	No
Ver el panel y todas las pestañas	Sí	Sí	Sí	Sí	Sí
Comience una prueba gratuita	Sí	No	No	No	No
Iniciar el descubrimiento de cargas de trabajo	No	Sí	Sí	Sí	No
Ver información de la licencia	Sí	Sí	Sí	Sí	Sí
Activar licencia	Sí	No	No	No	No
Ver anfitriones	Sí	Sí	Sí	Sí	Sí
Horarios:					
Activar horarios	Sí	Sí	Sí	Sí	No
Suspender horarios	Sí	Sí	Sí	Sí	No
Políticas y protección:					
Ver planes de protección	Sí	Sí	Sí	Sí	Sí
Crear, modificar o eliminar planes de protección	Sí	Sí	No	No	No
Restaurar cargas de trabajo	Sí	No	Sí	No	No
Crear, dividir o eliminar clones	Sí	No	No	Sí	No
Crear, modificar o eliminar una política	Sí	Sí	No	No	No
Informes:					
Ver informes	Sí	Sí	Sí	Sí	Sí
Crear informes	Sí	Sí	Sí	Sí	No

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Administrador de clones de Backup and Recovery	Visor de copias de seguridad y recuperación
Eliminar informes	Sí	No	No	No	No
Importar desde SnapCenter y administrar el host:					
Ver datos importados de SnapCenter	Sí	Sí	Sí	Sí	Sí
Importar datos desde SnapCenter	Sí	Sí	No	No	No
Administrar (migrar) host	Sí	Sí	No	No	No
Configurar ajustes:					
Configurar el directorio de registro	Sí	Sí	Sí	No	No
Asociar o eliminar credenciales de instancia	Sí	Sí	Sí	No	No
Cubos:					
Ver depósitos	Sí	Sí	Sí	Sí	Sí
Crear, editar o eliminar un depósito	Sí	Sí	No	No	No

Roles utilizados para acciones específicas de la carga de trabajo

La siguiente tabla indica las acciones que cada rol de NetApp Backup and Recovery puede realizar para cargas de trabajo específicas.

Cargas de trabajo de Kubernetes

Esta tabla indica las acciones que cada rol de NetApp Backup and Recovery puede realizar para acciones específicas de las cargas de trabajo de Kubernetes.

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Visor de copias de seguridad y recuperación
Ver clústeres, espacios de nombres, clases de almacenamiento y recursos de API	Sí	Sí	Sí	Sí

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Visor de copias de seguridad y recuperación
Agregar nuevos clústeres de Kubernetes	Sí	Sí	No	No
Actualizar las configuraciones del clúster	Sí	No	No	No
Eliminar clústeres de la administración	Sí	No	No	No
Ver aplicaciones	Sí	Sí	Sí	Sí
Crear y definir nuevas aplicaciones	Sí	Sí	No	No
Actualizar las configuraciones de la aplicación	Sí	Sí	No	No
Eliminar aplicaciones de la administración	Sí	Sí	No	No
Ver los recursos protegidos y el estado de la copia de seguridad	Sí	Sí	Sí	Sí
Cree copias de seguridad y proteja aplicaciones con políticas	Sí	Sí	No	No
Desproteger aplicaciones y eliminar copias de seguridad	Sí	Sí	No	No
Ver puntos de recuperación y resultados del visor de recursos	Sí	Sí	Sí	Sí
Restaurar aplicaciones desde puntos de recuperación	Sí	No	Sí	No
Ver las políticas de respaldo de Kubernetes	Sí	Sí	Sí	Sí
Crear políticas de respaldo de Kubernetes	Sí	Sí	Sí	No
Actualizar las políticas de respaldo	Sí	Sí	Sí	No

Característica y acción	Superadministrador de copias de seguridad y recuperación	Administrador de copias de seguridad y recuperación	Administrador de restauración de copias de seguridad y recuperación	Visor de copias de seguridad y recuperación
Eliminar políticas de copia de seguridad	Sí	Sí	Sí	No
Ver ganchos de ejecución y fuentes de ganchos	Sí	Sí	Sí	Sí
Crear ganchos de ejecución y fuentes de gancho	Sí	Sí	Sí	No
Actualizar los ganchos de ejecución y las fuentes de los ganchos	Sí	Sí	Sí	No
Eliminar ganchos de ejecución y fuentes de ganchos	Sí	Sí	Sí	No
Ver plantillas de gancho de ejecución	Sí	Sí	Sí	Sí
Crear plantillas de gancho de ejecución	Sí	Sí	Sí	No
Actualizar plantillas de gancho de ejecución	Sí	Sí	Sí	No
Eliminar plantillas de gancho de ejecución	Sí	Sí	Sí	No
Ver el resumen de la carga de trabajo y los paneles de análisis	Sí	Sí	Sí	Sí
Ver depósitos y destinos de almacenamiento de StorageGRID	Sí	Sí	Sí	Sí

Funciones de NetApp Disaster Recovery en la NetApp Console

Puede asignar los siguientes roles a los usuarios para brindarles acceso a NetApp Disaster Recovery dentro de la consola. Los roles de recuperación ante desastres le brindan la flexibilidad de asignar a los usuarios un rol específico para las tareas que necesitan realizar dentro de su organización. La forma de asignar roles depende de su propio negocio y de sus prácticas de gestión de almacenamiento.

La recuperación ante desastres utiliza los siguientes roles:

- **Administrador de recuperación ante desastres**: Realizar cualquier acción.
- **Administrador de conmutación por error de recuperación ante desastres**: realiza conmutaciones por

error y migraciones.

- **Administrador de aplicaciones de recuperación ante desastres**: crear planes de replicación. Modificar los planes de replicación. Iniciar pruebas de conmutación por error.
- **Visor de recuperación ante desastres**: Ver solo información.

La siguiente tabla indica las acciones que puede realizar cada rol.

Característica y acción	Administración de recuperación ante desastres	Administrador de conmutación por error de recuperación ante desastres	Administrador de aplicaciones de recuperación ante desastres	Visor de recuperación ante desastres
Ver el panel y todas las pestañas	Sí	Sí	Sí	Sí
Comience una prueba gratuita	Sí	No	No	No
Iniciar el descubrimiento de cargas de trabajo	Sí	No	No	No
Ver información de la licencia	Sí	Sí	Sí	Sí
Activar licencia	Sí	No	Sí	No
En la pestaña Sitios:				
Ver sitios	Sí	Sí	Sí	Sí
Agregar, modificar o eliminar sitios	Sí	No	No	No
En la pestaña Planes de replicación:				
Ver planes de replicación	Sí	Sí	Sí	Sí
Ver detalles del plan de replicación	Sí	Sí	Sí	Sí
Crear o modificar planes de replicación	Sí	Sí	Sí	No
Crear informes	Sí	No	No	No
Ver instantáneas	Sí	Sí	Sí	Sí
Realizar pruebas de conmutación por error	Sí	Sí	Sí	No
Realizar conmutaciones por error	Sí	Sí	No	No
Realizar conmutaciones por recuperación	Sí	Sí	No	No

Característica y acción	Administración de recuperación ante desastres	Administrador de conmutación por error de recuperación ante desastres	Administrador de aplicaciones de recuperación ante desastres	Visor de recuperación ante desastres
Realizar migraciones	Sí	Sí	No	No
En la pestaña Grupos de recursos:				
Ver grupos de recursos	Sí	Sí	Sí	Sí
Crear, modificar o eliminar grupos de recursos	Sí	No	Sí	No
En la pestaña Supervisión de trabajos:				
Ver trabajos	Sí	No	Sí	Sí
Cancelar trabajos	Sí	Sí	Sí	No

Roles de acceso de resiliencia contra ransomware para la NetApp Console

Los roles de resiliencia contra ransomware brindan a los usuarios acceso a NetApp Ransomware Resilience. Ransomware Resilience admite las siguientes funciones:

Roles de base

- Administrador de resiliencia contra ransomware: configure los ajustes de resiliencia contra ransomware; investigue y responda a las alertas de cifrado
- Visor de resiliencia contra ransomware: vea incidentes de cifrado, informes y configuraciones de detección

Roles de actividad de comportamiento del usuario"Detección de actividad sospechosa de usuarios" Las alertas proporcionan visibilidad de datos tales como eventos de actividad de archivos; estas alertas incluyen nombres de archivos y acciones de archivos (como leer, escribir, eliminar, cambiar nombre) realizadas por el usuario. Para limitar la visibilidad de estos datos, solo los usuarios con estos roles pueden administrar o ver estas alertas.

- Administrador de comportamiento del usuario de Ransomware Resilience: active la detección de actividad sospechosa de usuarios, investigue y responda a las alertas de actividad sospechosa de usuarios
- Visor de comportamiento del usuario de Ransomware Resilience: vea alertas de actividad sospechosa del usuario

> Los roles de comportamiento del usuario no son roles independientes; están diseñados para agregarse a los roles de administrador o espectador de Ransomware Resilience. Para obtener más información, consulte Roles de comportamiento del usuario.

Consulte las siguientes tablas para obtener descripciones detalladas de cada función.

Roles de base

La siguiente tabla describe las acciones disponibles para los roles de administrador y espectador de Ransomware Resilience.

Característica y acción	Administrador de resiliencia frente al ransomware	Visor de resiliencia contra ransomware
Ver el panel y todas las pestañas	Sí	Sí
En el panel, actualice el estado de la recomendación	Sí	No
Comience una prueba gratuita	Sí	No
Iniciar el descubrimiento de cargas de trabajo	Sí	No
Iniciar el redescubrimiento de cargas de trabajo	Sí	No
En la pestaña Proteger:		
Agregar, modificar o eliminar planes de protección para políticas de *cifrado*	Sí	No
Proteger las cargas de trabajo	Sí	No
Identifique la exposición a datos confidenciales con la clasificación de datos	Sí	No
Enumere los planes de protección y los detalles	Sí	Sí
Lista de grupos de protección	Sí	Sí
Ver detalles del grupo de protección	Sí	Sí
Crear, editar o eliminar grupos de protección	Sí	No
Descargar datos	Sí	Sí
En la pestaña Alertas:		
Ver alertas de cifrado y detalles de alertas	Sí	Sí
Editar el estado del incidente de cifrado	Sí	No
Marcar alerta de cifrado para recuperación	Sí	No
Ver detalles del incidente de cifrado	Sí	Sí

Característica y acción	Administrador de resiliencia frente al ransomware	Visor de resiliencia contra ransomware
Descartar o resolver incidentes de cifrado	Sí	No
Obtenga la lista completa de archivos afectados en el evento de cifrado	Sí	No
Descargar datos de alertas de eventos de cifrado	Sí	Sí
Bloquear usuario (con configuración del agente de Workload Security)	Sí	No
En la pestaña Recuperar:		
Descargar archivos afectados por el evento de cifrado	Sí	No
Restaurar la carga de trabajo a partir de un evento de cifrado	Sí	No
Descargar datos de recuperación del evento de cifrado	Sí	Sí
Descargar informes de eventos de cifrado	Sí	Sí
En la pestaña Configuración:		
Agregar o modificar destinos de copia de seguridad	Sí	No
Lista de destinos de copia de seguridad	Sí	Sí
Ver objetivos SIEM conectados	Sí	Sí
Agregar o modificar objetivos SIEM	Sí	No
Configurar el simulacro de preparación	Sí	No
Iniciar, reiniciar o editar el simulacro de preparación	Sí	No
Revisar el estado del simulacro de preparación	Sí	Sí
Actualizar la configuración de descubrimiento	Sí	No
Ver configuración de descubrimiento	Sí	Sí
En la pestaña Informes:		
Descargar informes	Sí	Sí

Roles de comportamiento del usuario

Para configurar los ajustes de comportamiento de usuario sospechoso y responder a las alertas, un usuario debe tener el rol de administrador de comportamiento de usuario de Ransomware Resilience. Para ver únicamente alertas de comportamiento sospechoso del usuario, el usuario debe tener el rol de visualizador de comportamiento del usuario de Ransomware Resilience.

Los roles de comportamiento del usuario deben otorgarse a los usuarios con privilegios de administrador o espectador de Ransomware Resilience existentes que necesitan acceso a"Configuración y alertas de actividad de usuario sospechosa" . Un usuario con el rol de administrador de Ransomware Resilience, por ejemplo, debería recibir el rol de administrador de comportamiento de usuario de Ransomware Resilience para configurar agentes de actividad de usuario y bloquear o desbloquear usuarios. El rol de administrador de comportamiento del usuario de Ransomware Resilience no debe otorgarse a un visor de Ransomware Resilience.

Para activar la detección de actividad de usuarios sospechosos, debe tener el rol de administrador de la organización de la consola.

La siguiente tabla describe las acciones disponibles para los roles de administrador y espectador del comportamiento del usuario de Ransomware Resilience.

Característica y acción	Comportamiento del usuario de Resiliencia ante Ransomware	Visor del comportamiento del usuario de Ransomware Resilience
En la pestaña Configuración:		
Crear, modificar o eliminar un agente de actividad del usuario	Sí	No
Crear o eliminar el conector del directorio de usuarios	Sí	No
Pausar o reanudar el recopilador de datos	Sí	No
Realizar un simulacro de preparación ante una violación de datos	Sí	No
En la pestaña Proteger:		
Agregar, modificar o eliminar planes de protección para políticas de *comportamiento sospechoso de usuarios*	Sí	No
En la pestaña Alertas:		
Ver alertas de actividad del usuario y detalles de las alertas	Sí	Sí
Editar el estado del incidente de actividad del usuario	Sí	No
Marcar la alerta de actividad del usuario para recuperación	Sí	No
Ver detalles de incidentes de actividad del usuario	Sí	Sí

Característica y acción	Comportamiento del usuario de Resiliencia ante Ransomware	Visor del comportamiento del usuario de Ransomware Resilience
Descartar o resolver incidentes de actividad del usuario	Sí	No
Obtenga una lista completa de archivos afectados por usuarios sospechosos	Sí	Sí
Descargar datos de alertas de eventos de actividad del usuario	Sí	Sí
Bloquear o desbloquear usuario	Sí	No
En la pestaña Recuperar:		
Descargar archivos afectados por el evento de actividad del usuario	Sí	No
Restaurar la carga de trabajo a partir del evento de actividad del usuario	Sí	No
Descargar datos de recuperación del evento de actividad del usuario	Sí	Sí
Descargar informes de eventos de actividad del usuario	Sí	Sí

API de identidad y acceso

Identificadores de organizaciones y proyectos

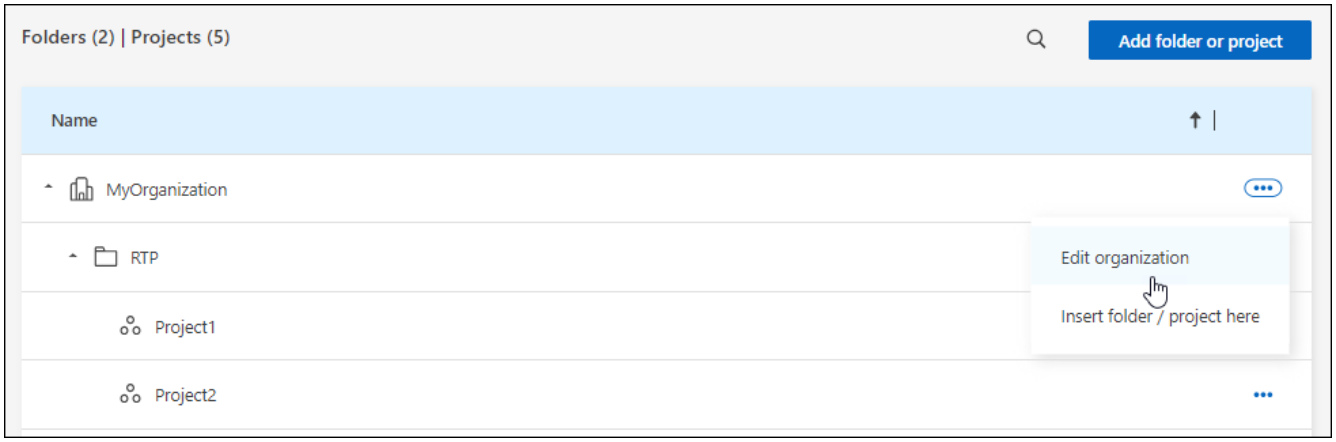
Su organización de la NetApp Console tiene un nombre y un ID. Puede elegir un nombre para su organización para ayudar a identificarla. Es posible que también necesites recuperar el ID de la organización para ciertas integraciones.

Cambie el nombre de su organización

Puede cambiar el nombre de su organización. Esto es útil si apoyas a más de una organización.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Organización**.
3. Desde la página **Organización**, navegue hasta la primera fila de la tabla, seleccione ••• y luego seleccione **Editar organización**.



4. Ingrese un nuevo nombre para la organización y seleccione **Aplicar**.

Obtener el ID de la organización

El ID de la organización se utiliza para ciertas integraciones con la consola.

Puede ver el ID de la organización desde la página Organizaciones y copiarlo al portapapeles según sus necesidades.

Pasos

1. Seleccione **Administración > Identidad y acceso** > **Organización**.
2. En la página **Organización**, busque el ID de su organización en la barra de resumen y cópielo al portapapeles. Puedes guardarlo para usarlo más tarde o copiarlo directamente donde necesites usarlo.

Obtener el ID de un proyecto

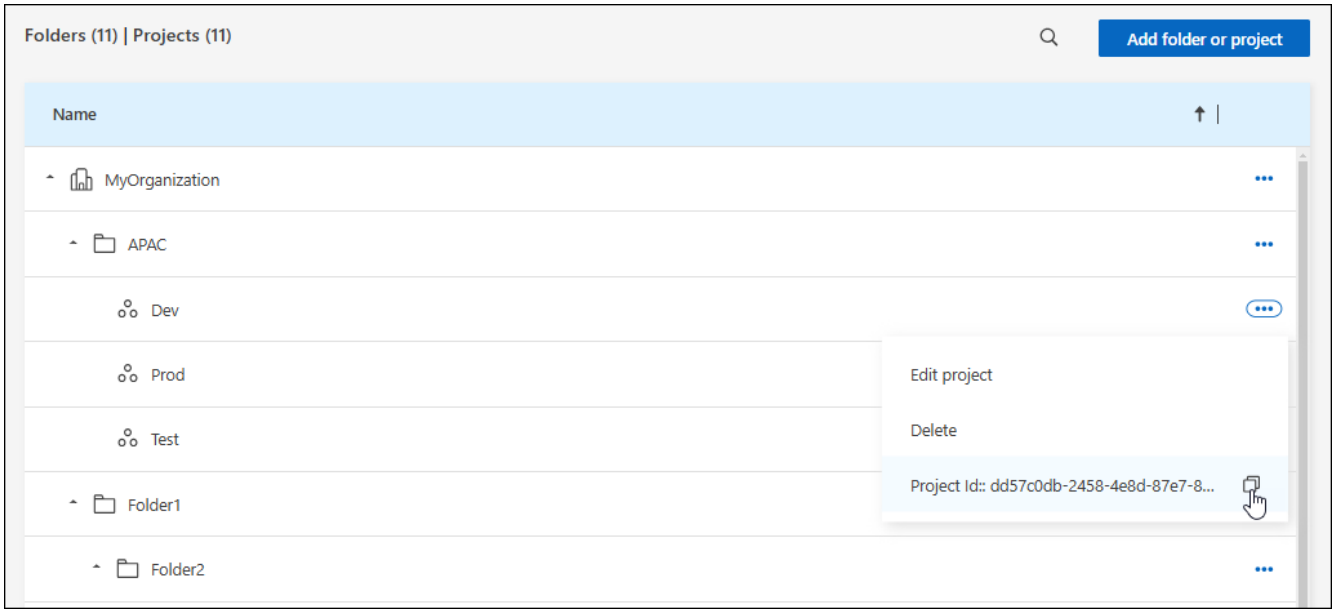
Necesitarás obtener el ID de un proyecto si estás usando la API. Por ejemplo, al crear un sistema Cloud Volumes ONTAP .

Pasos

1. Desde la página **Organización**, navegue hasta un proyecto en la tabla y seleccione •••

   Se muestra el ID del proyecto.

2. Para copiar el ID, seleccione el botón copiar.



Información relacionada

- "Aprenda sobre la gestión de identidad y acceso"
- "Comience con la identidad y el acceso"
- "Conozca la API para identidad y acceso"

Seguridad y cumplimiento

Federación de identidades

Habilite el inicio de sesión único mediante la federación de identidades con la NetApp Console

El inicio de sesión único (federación) simplifica el proceso de inicio de sesión y mejora la seguridad al permitir que los usuarios inicien sesión en la NetApp Console con sus credenciales corporativas. Puede habilitar el inicio de sesión único (SSO) con su proveedor de identidad (IdP) o con el sitio de soporte de NetApp .

Rol requerido

Administrador de la organización, administrador de la federación, visor de la federación."Obtenga más información sobre los roles de acceso."

Inicio de sesión único con NetApp Support Site

La federación con el sitio de soporte de NetApp permite a los usuarios iniciar sesión en la consola, Active IQ Digital Advisor y otras aplicaciones asociadas utilizando las mismas credenciales.

Si se federa con el sitio de soporte de NetApp , no podrá federarse también con su proveedor de gestión de identidad corporativa. Elija cuál funciona mejor para su organización.

Pasos

1. Descargue y complete el "Formulario de solicitud de federación de NetApp" .
2. Envíe el formulario a la dirección de correo electrónico especificada en el formulario.

El equipo de soporte de NetApp revisa y procesa su solicitud.

Inicio de sesión único con tu proveedor de identidades

Puede configurar una conexión federada con su proveedor de identidad para habilitar el inicio de sesión único (SSO) para la consola. El proceso implica configurar su proveedor de identidad para que confíe en NetApp como proveedor de servicios y luego crear la conexión en la consola.

Si anteriormente configuró la federación usando NetApp Cloud Central (una aplicación externa a la consola), debe importar su federación usando la página Federación para administrarla dentro de la consola."Aprenda cómo importar su federación."

Proveedores de identidad compatibles

NetApp admite los siguientes protocolos y proveedores de identidad para la federación:

Protocolos

- Proveedores de identidad de lenguaje de marcado de aserción de seguridad (SAML)
- Servicios de federación de Active Directory (AD FS)

Proveedores de identidad

- Identificador de Microsoft Entra
- Federación de ping

Flujo de trabajo de la Federación con la NetApp Console

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para confiar en NetApp como proveedor de servicios. Luego, puede crear una conexión en la consola que utilice la configuración del proveedor de identidad.

Puedes federarlo con tu dominio de correo electrónico o con un dominio diferente que sea de tu propiedad. Para federarse con un dominio diferente de su dominio de correo electrónico, primero verifique que usted es el propietario del dominio.

1 Verifica tu dominio (si no utilizas tu dominio de correo electrónico)

Para federarse con un dominio diferente a su dominio de correo electrónico, verifique que sea su propietario. Puede federar su dominio de correo electrónico sin realizar pasos adicionales.

2 Configure su IdP para confiar en NetApp como proveedor de servicios

Configure su proveedor de identidad para que confíe en NetApp creando una nueva aplicación y proporcionando detalles como la URL de ACS, el ID de entidad u otra información de credenciales. La información del proveedor de servicios varía según el proveedor de identidad, por lo que consulte la documentación de su proveedor de identidad específico para obtener más detalles. Necesitará trabajar con el administrador de su IdP para completar este paso.

3 Crear la conexión federada en la consola

Proporcione la URL o el archivo de metadatos SAML de su proveedor de identidad para crear la conexión. Esta información se utiliza para establecer la relación de confianza entre la consola y su proveedor de identidad. La información que proporciones dependerá del IdP que estés utilizando. Por ejemplo, si utiliza Microsoft Entra ID, deberá proporcionar el ID de cliente, el secreto y el dominio.

4 Pruebe su federación en la consola

Pruebe su conexión federada antes de habilitarla. Utilice la opción de prueba en la página Federación en la Consola para verificar que su usuario de prueba pueda autenticarse correctamente. Si la prueba es exitosa, puedes habilitar la conexión.

5 Habilite su conexión en la Consola

Después de habilitar la conexión, los usuarios pueden iniciar sesión en la consola utilizando sus credenciales corporativas.

Revise el tema de su respectivo protocolo o IdP para comenzar:

- "Configurar una conexión federada con AD FS"
- "Configurar una conexión federada con Microsoft Entra ID"
- "Configurar una conexión federada con PingFederate"
- "Configurar una conexión federada con un proveedor de identidad SAML"

Verificación de dominio

Verifique el dominio de correo electrónico para su conexión federada

Si desea federarse con un dominio diferente a su dominio de correo electrónico, primero debe verificar que es el propietario del dominio. Sólo se pueden utilizar dominios verificados para la federación.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Para verificar su dominio es necesario agregar un registro TXT a la configuración de DNS de su dominio. Este registro se utiliza para demostrar que usted es el propietario del dominio y permite que la NetApp Console confíe en el dominio para la federación. Es posible que necesite coordinar con su administrador de TI o de red para completar este paso.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.
4. Seleccione **Verificar propiedad del dominio**.
5. Ingrese el dominio que desea verificar y seleccione **Continuar**.
6. Copie el registro TXT que se proporciona.

7. Vaya a la configuración de DNS de su dominio y configure el valor TXT que se proporcionó como registro TXT para su dominio. Trabaje con su administrador de TI o de red si es necesario.
8. Después de agregar el registro TXT, regrese a la Consola y seleccione **Verificar**.

Configurar federaciones

Federar la NetApp Console con los Servicios de federación de Active Directory (AD FS)

Federe sus Servicios de federación de Active Directory (AD FS) con la NetApp Console para habilitar el inicio de sesión único (SSO) para la NetApp Console. Esto permite a los usuarios iniciar sesión en la consola utilizando sus credenciales corporativas.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Puede federarse con su IdP corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero, configure el proveedor de identidad para que confíe en la NetApp Console como proveedor de servicios. Luego, crea una conexión en la consola utilizando la configuración de tu proveedor de identidad.

Puede configurar la federación con su servidor AD FS para habilitar el inicio de sesión único (SSO) para NetApp Console. El proceso implica configurar AD FS para que confíe en la consola como proveedor de servicios y luego crear la conexión en la NetApp Console.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
    a. Elija si desea utilizar un dominio verificado o su dominio de correo electrónico. El dominio de correo electrónico es el dominio asociado con la cuenta con la que ha iniciado sesión.
    b. Introduzca el nombre de la federación que está configurando.
    c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.
6. Para su método de conexión, elija **Protocolo** y luego seleccione **Servicios de federación de Active Directory (AD FS)**.
7. Seleccione **Siguiente**.
8. Cree una relación de confianza de usuario autenticado en su servidor AD FS. Puede usar PowerShell o configurarlo manualmente en su servidor AD FS. Consulte la documentación de AD FS para obtener detalles sobre cómo crear una relación de confianza entre usuarios.
    a. Cree la confianza mediante PowerShell mediante el siguiente script:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]
::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
auth0/master/AD FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
cloud-account.auth0.com/login/callback"
```

b. Alternativamente, puede crear la confianza manualmente en la consola de administración de AD FS. Utilice los siguientes valores de la NetApp Console al crear la confianza:

   - Al crear el identificador de confianza confiable, utilice el valor **YOUR_TENANT**: `netapp-cloud-account`
   - Cuando seleccione **Habilitar soporte para WS-Federation**, utilice el valor **YOUR_AUTH0_DOMAIN**: `netapp-cloud-account.auth0.com`

c. Después de crear la confianza, copie la URL de metadatos de su servidor AD FS o descargue el archivo de metadatos de federación. Necesitará esta URL o archivo para completar la conexión en la consola.

NetApp recomienda utilizar la URL de metadatos para permitir que la NetApp Console recupere automáticamente la última configuración de AD FS. Si descarga el archivo de metadatos de federación, deberá actualizarlo manualmente en la NetApp Console cada vez que haya cambios en su configuración de AD FS.

9. Regrese a la consola y seleccione **Siguiente** para crear la conexión.
10. Cree la conexión con AD FS.
    a. Ingrese la **URL de AD FS** que copió de su servidor de AD FS en el paso anterior o cargue el archivo de metadatos de federación que descargó de su servidor de AD FS.
11. Seleccione **Crear conexión**. La creación de la conexión puede tardar unos segundos.
12. Seleccione **Siguiente**.
13. Seleccione **Probar conexión** para probar su conexión. Se le dirigirá a una página de inicio de sesión para su servidor IdP. Inicie sesión con sus credenciales de IdP. Después de iniciar sesión, regrese a la Consola para habilitar la conexión.

    Al utilizar la consola en modo restringido, copie la URL en una ventana de incógnito del navegador o en un navegador separado para iniciar sesión en su IdP.

14. En la consola, seleccione **Siguiente** para revisar la página de resumen.
15. Configurar notificaciones.

    Elija entre siete días o 30 días. El sistema envía notificaciones de vencimiento por correo electrónico y las muestra en la consola a cualquier usuario con los siguientes roles: superadministrador, administrador de la organización, administrador de la federación y visor de la federación.

16. Revise los detalles de la federación y luego seleccione **Habilitar federación**.
17. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios inician sesión en la NetApp Console con sus credenciales corporativas.

Federar la NetApp Console con el ID de Microsoft Entra

Fedérese con su proveedor de IdP de Microsoft Entra ID para habilitar el inicio de sesión único (SSO) para la NetApp Console. Esto permite a los usuarios iniciar sesión utilizando sus credenciales corporativas.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Puede federarse con su IdP corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para confiar en NetApp como proveedor de servicios. Luego, puede crear una conexión en la consola que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con Microsoft Entra ID para habilitar el inicio de sesión único (SSO) para la consola. El proceso implica configurar su ID de Microsoft Entra para confiar en la consola como proveedor de servicios y luego crear la conexión en la consola.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.

Detalles del dominio

1. Introduzca los detalles de su dominio:
   a. Elija si desea utilizar un dominio verificado o su dominio de correo electrónico. El dominio de correo electrónico es el dominio asociado con la cuenta con la que ha iniciado sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
2. Seleccione **Siguiente**.

Método de conexión

1. Para su método de conexión, elija **Proveedor** y luego seleccione **Microsoft Entra ID**.
2. Seleccione **Siguiente**.

Instrucciones de configuración

1. Configure su ID de Microsoft Entra para confiar en NetApp como proveedor de servicios. Debe realizar este paso en su servidor Microsoft Entra ID.
   a. Utilice los siguientes valores al registrar su aplicación Microsoft Entra ID para confiar en la consola:
      - Para la **URL de redirección**, utilice `https://services.cloud.netapp.com`
      - Para la **URL de respuesta**, utilice `https://netapp-cloud-account.auth0.com/login/callback`

b. Cree un secreto de cliente para su aplicación Microsoft Entra ID. Necesitará proporcionar el ID del cliente, el secreto del cliente y el nombre de dominio de Entra ID para completar la federación.

2. Regrese a la consola y seleccione **Siguiente** para crear la conexión.

Crear conexión

1. Crear la conexión con Microsoft Entra ID
   a. Ingrese el ID de cliente y el secreto de cliente que creó en el paso anterior.
   b. Introduzca el nombre de dominio de Microsoft Entra ID.
2. Seleccione **Crear conexión**. El sistema crea la conexión en unos segundos.

Probar y habilitar la conexión

1. Seleccione **Siguiente**.
2. Seleccione **Probar conexión** para probar su conexión. Se le dirigirá a una página de inicio de sesión para su servidor IdP. Inicie sesión con sus credenciales de IdP. Después de iniciar sesión, regrese a la Consola para habilitar la conexión.

   Al utilizar la consola en modo restringido, copie la URL en una ventana de incógnito del navegador o en un navegador separado para iniciar sesión en su IdP.

3. En la consola, seleccione **Siguiente** para revisar la página de resumen.
4. Configurar notificaciones.

   Elija entre siete días o 30 días. El sistema envía notificaciones de vencimiento por correo electrónico y las muestra en la consola a cualquier usuario con los siguientes roles: superadministrador, administrador de la organización, administrador de la federación y visor de la federación.

5. Revise los detalles de la federación y luego seleccione **Habilitar federación**.
6. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios inician sesión en la NetApp Console con sus credenciales corporativas.

Federar la NetApp Console con PingFederate

Fedérese con su proveedor de IdP de PingFederate para habilitar el inicio de sesión único (SSO) para la NetApp Console. Esto permite a los usuarios iniciar sesión utilizando sus credenciales corporativas.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Puede federarse con su IdP corporativo o con el sitio de soporte de NetApp . NetApp recomienda elegir uno u otro, pero no ambos.

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para confiar en NetApp como proveedor de servicios. Luego, puede crear una conexión en la consola que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con PingFederate para habilitar el inicio de sesión único (SSO) para la consola. El proceso implica configurar su servidor PingFederate para que confíe en la consola como proveedor de servicios y luego crear la conexión en la consola.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
   a. Elija si desea utilizar un dominio verificado o su dominio de correo electrónico. El dominio de correo electrónico es el dominio asociado con la cuenta con la que ha iniciado sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.
6. Para su método de conexión, elija **Proveedor** y luego seleccione **PingFederate**.
7. Seleccione **Siguiente**.
8. Configure su servidor PingFederate para confiar en NetApp como proveedor de servicios. Debes realizar este paso en tu servidor PingFederate.
   a. Utilice los siguientes valores al configurar PingFederate para confiar en la NetApp Console:
      - Para la **URL de respuesta** o la **URL del servicio de consumidor de afirmaciones (ACS)**, utilice `https://netapp-cloud-account.auth0.com/login/callback`
      - Para la **URL de cierre de sesión**, utilice `https://netapp-cloud-account.auth0.com/logout`
      - Para **ID de audiencia/entidad**, utilice `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` donde <fed-domain-name-pingfederate> es el nombre de dominio de la federación. Por ejemplo, si su dominio es `example.com` , el ID de audiencia/entidad sería `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .
   b. Copie la URL del servidor PingFederate. Necesitará esta URL al crear la conexión en la consola.
   c. Descargue el certificado X.509 de su servidor PingFederate. Debe estar en formato PEM codificado en Base64 (.pem, .crt, .cer).
9. Regrese a la consola y seleccione **Siguiente** para crear la conexión.
10. Crea la conexión con PingFederate
    a. Ingrese la URL del servidor PingFederate que copió en el paso anterior.
    b. Cargue el certificado de firma X.509. El certificado debe estar en formato PEM, CER o CRT.
11. Seleccione **Crear conexión**. El sistema crea la conexión en unos segundos.
12. Seleccione **Siguiente**.
13. Seleccione **Probar conexión** para probar su conexión. Se le dirigirá a una página de inicio de sesión para su servidor IdP. Inicie sesión con sus credenciales de IdP. Después de iniciar sesión, regrese a la Consola para habilitar la conexión.

> Al utilizar la consola en modo restringido, copie la URL en una ventana de incógnito del navegador o en un navegador separado para iniciar sesión en su IdP.

14. En la consola, seleccione **Siguiente** para revisar la página de resumen.
15. Configurar notificaciones.

    Elija entre siete días o 30 días. El sistema envía notificaciones de vencimiento por correo electrónico y las muestra en la consola a cualquier usuario con los siguientes roles: superadministrador, administrador de la organización, administrador de la federación y visor de la federación.

16. Revise los detalles de la federación y luego seleccione **Habilitar federación**.
17. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios inician sesión en la NetApp Console con sus credenciales corporativas.

Federarse con un proveedor de identidad SAML

Fedérese con su proveedor de IdP SAML 2.0 para habilitar el inicio de sesión único (SSO) para la consola NEtApp. Esto permite a los usuarios iniciar sesión utilizando sus credenciales corporativas.

Rol requerido

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

Puede federarse con su IdP corporativo o con el sitio de soporte de NetApp . No es posible federarse con ambos.

NetApp solo admite el inicio de sesión único (SSO) iniciado por el proveedor de servicios (SP). Primero debe configurar el proveedor de identidad para confiar en NetApp como proveedor de servicios. Luego, puede crear una conexión en la consola que utilice la configuración del proveedor de identidad.

Puede configurar una conexión federada con su proveedor de SAML 2.0 para habilitar el inicio de sesión único (SSO) para la consola. El proceso implica configurar su proveedor para que confíe en NetApp como proveedor de servicios y luego crear la conexión en la consola.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Federación** para ver la página **Federaciones**.
3. Seleccione **Configurar nueva federación**.
4. Introduzca los detalles de su dominio:
   a. Elija si desea utilizar un dominio verificado o su dominio de correo electrónico. El dominio de correo electrónico es el dominio asociado con la cuenta con la que ha iniciado sesión.
   b. Introduzca el nombre de la federación que está configurando.
   c. Si elige un dominio verificado, seleccione el dominio de la lista.
5. Seleccione **Siguiente**.
6. Para su método de conexión, elija **Protocolo** y luego seleccione **Proveedor de identidad SAML**.
7. Seleccione **Siguiente**.
8. Configure su proveedor de identidad SAML para confiar en NetApp como proveedor de servicios. Debe realizar este paso en su servidor proveedor SAML.

a. Asegúrese de que su IdP tenga el atributo `email` establecer en la dirección de correo electrónico del usuario. Esto es necesario para que la consola identifique correctamente a los usuarios:

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. Utilice los siguientes valores al registrar su aplicación SAML con la consola:
   - Para la **URL de respuesta** o la **URL del servicio de consumidor de afirmaciones (ACS)**, utilice `https://netapp-cloud-account.auth0.com/login/callback`
   - Para la **URL de cierre de sesión**, utilice `https://netapp-cloud-account.auth0.com/logout`
   - Para **ID de audiencia/entidad**, utilice `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` donde <fed-domain-name-saml> es el nombre de dominio que desea utilizar para la federación. Por ejemplo, si su dominio es `example.com` , el ID de audiencia/entidad sería `urn:auth0:netapp-cloud-account:fed-example-com-samlp` .
2. Después de crear la confianza, copie los siguientes valores de su servidor de proveedor SAML:
   - URL de inicio de sesión
   - URL de cierre de sesión (opcional)
3. Descargue el certificado X.509 de su servidor proveedor SAML. Debe estar en formato PEM, CER o CRT.
   a. Regrese a la consola y seleccione **Siguiente** para crear la conexión.
   b. Crear la conexión con SAML.
4. Introduzca la **URL de inicio de sesión** de su servidor SAML.
5. Cargue el certificado X.509 que descargó de su servidor de proveedor SAML.
6. Opcionalmente, ingrese la **URL de cierre de sesión** de su servidor SAML.
   a. Seleccione **Crear conexión**. El sistema crea la conexión en unos segundos.
   b. Seleccione **Siguiente**.
   c. Seleccione **Probar conexión** para probar su conexión. Se le dirigirá a una página de inicio de sesión para su servidor IdP. Inicie sesión con sus credenciales de IdP. Después de iniciar sesión, regrese a la Consola para habilitar la conexión.

      Al utilizar la consola en modo restringido, copie la URL en una ventana de incógnito del navegador o en un navegador separado para iniciar sesión en su IdP.

   d. En la consola, seleccione **Siguiente** para revisar la página de resumen.
   e. Configurar notificaciones.

Elija entre siete días o 30 días. El sistema envía notificaciones de vencimiento por correo electrónico y las muestra en la consola a cualquier usuario con los siguientes roles: superadministrador, administrador de la organización, administrador de la federación y visor de la federación.

f. Revise los detalles de la federación y luego seleccione **Habilitar federación**.

g. Seleccione **Finalizar** para completar el proceso.

Después de habilitar la federación, los usuarios inician sesión en la NetApp Console con sus credenciales corporativas.

Administrar federaciones

Administrar federaciones en la NetApp Console

Puede administrar su federación en la NetApp Console. Puede desactivarlo, actualizar credenciales vencidas, así como desactivarlo si ya no lo necesita.

Roles requeridos

El rol de administrador de la federación es necesario para crear y administrar federaciones. El espectador de la Federación puede ver la página de la Federación."Obtenga más información sobre los roles de acceso."

También puede agregar un dominio verificado adicional a una federación existente, lo que le permite utilizar múltiples dominios para su conexión federada.

- Si configuró la federación mediante NetApp Cloud Central, impórtela a través de la página **Federación** para administrarla en la consola."Aprenda a importar su federación"
- Puede ver eventos de administración de la federación, como habilitar, deshabilitar y actualizar federaciones en la página Auditoría. "Obtenga más información sobre la supervisión de operaciones en la NetApp Console."

Habilitar una federación

Si ha creado una federación pero no está habilitada, puede habilitarla a través de la página **Federación**. Habilitar una federación permite que los usuarios asociados con la federación inicien sesión en la Consola usando sus credenciales corporativas. Cree y pruebe la federación con éxito antes de habilitarla.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones ••• junto a la federación que desea habilitar y seleccione **Habilitar**.

Agregar un dominio verificado a una federación existente

Puede agregar un dominio verificado a una federación existente en la Consola para usar múltiples dominios con el mismo proveedor de identidad (IdP).

Debes haber verificado ya el dominio en la consola antes de poder agregarlo a una federación. Si aún no ha verificado el dominio, puede hacerlo siguiendo los pasos en"Verifica tu dominio en la consola" .

Pasos

1. Seleccione **Administración > Identidad y acceso**.

2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones junto a la federación a la que desea agregar un dominio verificado y seleccione **Actualizar dominios**. El cuadro de diálogo **Actualizar dominios** muestra el dominio ya asociado con esta federación.
4. Seleccione un dominio verificado de la lista de dominios disponibles.
5. Seleccione **Actualizar**. Los nuevos usuarios del dominio pueden obtener acceso a la consola federada en 30 segundos.

Actualización de una conexión federada que está a punto de expirar

Puede actualizar los detalles de una federación en la Consola. Por ejemplo, necesitará actualizar la federación si las credenciales, como un certificado o un secreto de cliente, expiran. Cuando sea necesario, actualice la fecha de notificación para recordarle que debe actualizar la conexión antes de que expire.

Actualice la consola primero antes de actualizar su IdP para evitar problemas de inicio de sesión. Manténgase conectado a la consola durante el proceso.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones (tres puntos verticales) junto a la federación que desea actualizar y seleccione **Actualizar federación**.
4. Actualice los detalles de la federación según sea necesario.
5. Seleccione **Actualizar**.

Probar una federación existente

Pruebe la conexión de una federación existente para verificar que funciona. Esto puede ayudarle a identificar cualquier problema con la federación y solucionarlo.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones junto a la federación a la que desea agregar un dominio verificado y seleccione **Probar conexión**.
4. Seleccione **Prueba**. El sistema le solicita que inicie sesión con sus credenciales corporativas. Si la conexión es exitosa, será redirigido a la NetApp Console. Si falla la conexión, verá un mensaje de error que indica el problema con la federación.
5. Seleccione **Listo** para regresar a la pestaña **Federación**.

Deshabilitar una federación

Si ya no necesita una federación, puede desactivarla. Esto evita que los usuarios asociados a la federación inicien sesión en la consola utilizando sus credenciales corporativas. Puede volver a habilitar la federación más tarde si es necesario.

Deshabilite una federación antes de eliminarla, como por ejemplo al desmantelar el IdP o discontinuar la federación. Esto le permitirá volver a habilitarlo más tarde si es necesario.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione el menú de acciones junto a la federación a la que desea agregar un dominio verificado y seleccione **Deshabilitar**.

Eliminar una federación

Si ya no necesita una federación, puede eliminarla. Esto elimina la federación y evita que cualquier usuario asociado con la federación inicie sesión en la consola usando sus credenciales corporativas. Por ejemplo, si se está desmantelando el IdP o si la federación ya no es necesaria.

No es posible recuperar una federación después de eliminarla. Debes crear una nueva federación.

Debes deshabilitar una federación antes de poder eliminarla. No es posible recuperar una federación después de eliminarla.

Pasos

1. Seleccione **Administración > Identidad y acceso** .
2. Seleccione **Federaciones** para ver la página **Federaciones**.
3. Seleccione el menú de acciones junto a la federación a la que desea agregar un dominio verificado y seleccione **Eliminar**.

Importe su federación a la NetApp Console

Si previamente ha configurado la federación a través de NetApp Cloud Central (una aplicación externa a la NetApp Console), la página Federación le solicitará que importe su conexión federada existente a la consola para que pueda administrarla en la nueva interfaz. Luego podrá aprovechar las últimas mejoras sin tener que recrear su conexión federada.

Después de importar su federación existente, puede administrarla desde la página **Federaciones**."Obtenga más información sobre la gestión de federaciones."

Rol requerido

Administrador de la organización o administrador de la federación."Obtenga más información sobre los roles de acceso."

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Federación**.
3. Seleccione **Importar federación**.

Aplicar permisos de ONTAP para la Vista avanzada de ONTAP (Administrador del sistema ONTAP)

De forma predeterminada, las credenciales del agente de la consola permiten a los usuarios acceder a la Vista avanzada (ONTAP System Manager). En su lugar, puede

solicitar a los usuarios sus credenciales de ONTAP . Esto garantiza que los permisos de ONTAP de un usuario se apliquen cuando trabaja con clústeres de ONTAP tanto en Cloud Volumes ONTAP como en clústeres locales de ONTAP .

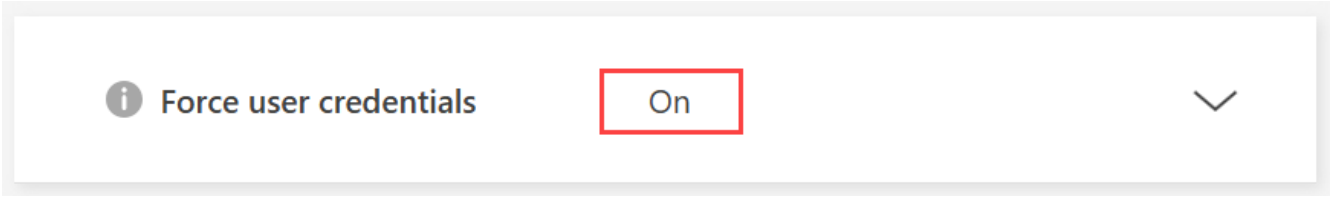
Debe tener el rol de administrador de la organización para editar la configuración del agente de la consola.

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. Expande la opción **Forzar Credenciales**.
4. Seleccione la casilla de verificación para habilitar la opción **Forzar credenciales** y luego seleccione **Guardar**.
5. Verifique que la opción **Forzar Credenciales** esté habilitada.



Habilitar el modo de solo lectura para una organización de NetApp Console

Como medida de seguridad, puede habilitar el modo de solo lectura para su organización de NetApp Console . En el modo de solo lectura, los usuarios pueden ver recursos y configuraciones, pero no pueden realizar cambios.

En el modo de solo lectura, los usuarios con roles de administrador deben elevar manualmente sus permisos para realizar cambios, lo que garantiza que los cambios sean intencionales.

Roles de acceso requeridos

Superadministrador o administrador de la organización.

Habilite el modo de solo lectura para su organización de la consola

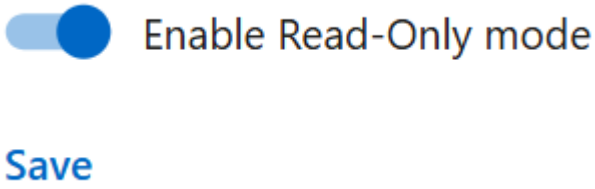
Habilite el modo de solo lectura para restringir los cambios en la organización de su consola. Todos los usuarios aún pueden ver los recursos. Los usuarios con roles de administrador no pueden realizar ninguna acción en la consola sin elevar manualmente sus permisos.

Cuando el modo de solo lectura está habilitado, los usuarios ven un banner que les notifica que la organización está en modo de solo lectura. Los usuarios deben ir a Configuración de usuario para elevar su rol.

Pasos

1. Seleccione **Administración > Identidad y acceso**.

2. Desde la pestaña **Organizaciones**, seleccione **Editar configuración de la organización** para la organización que desea configurar en modo de solo lectura.
3. En la sección **Modo de solo lectura**, habilite el modo de solo lectura moviendo el interruptor a la posición **Activado** y luego seleccione **Guardar**.



Regístrese en NetApp Console como administrador inicial de la organización

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

Pasos

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

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

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

      Sólo se permiten caracteres ingleses en el formulario de registro.

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

      Verifique su dirección de correo electrónico para completar el registro.

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

+ Como administrador por primera vez, siga el proceso guiado para agregar almacenamiento, crear un agente de consola y más. "Obtenga información sobre cómo utilizar el Asistente de consola."

Próximos pasos

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

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

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

Pasos

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

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

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

      Sólo se permiten caracteres ingleses en el formulario de registro.

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

      Verifique su dirección de correo electrónico para completar el registro.

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

Próximos pasos

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

Gestionar las asociaciones de la organización

Asociaciones de organizaciones en NetApp Console

La creación de asociaciones entre organizaciones en la NetApp Console permite a los socios administrar de forma segura los recursos de NetApp a través de los límites organizacionales, agilizando la colaboración y mejorando la seguridad.

Roles requeridos

Administración de asociaciones"Obtenga más información sobre los roles de acceso."

Las asociaciones permiten la gestión segura de los recursos de NetApp en todas las organizaciones mediante relaciones basadas en roles en la consola. La organización iniciadora concede acceso a sus recursos, mientras que la organización receptora proporciona los usuarios o las cuentas de servicio a los que se les concederá acceso. Las asociaciones se establecen a través de un flujo de trabajo de autoservicio, que brinda a la organización iniciadora control total sobre qué recursos se comparten, qué roles se asignan y la capacidad de incorporar, administrar o revocar el acceso de los socios según sea necesario.

Los clientes pueden autorizar a los MSP o revendedores a administrar entornos NetApp sin necesidad de configuraciones complicadas. Los clientes pueden controlar a qué clústeres pueden acceder los socios y qué roles tienen, y pueden revocar el acceso en cualquier momento para mantener la seguridad y el cumplimiento.

Como socio, obtiene visibilidad y control centralizados en todos los entornos de los clientes. Puede cambiar fácilmente a la organización de un cliente para administrar recursos, ejecutar servicios de datos y monitorear la salud dentro de límites definidos, lo que reduce las herramientas personalizadas y garantiza la alineación con las políticas de cada cliente.

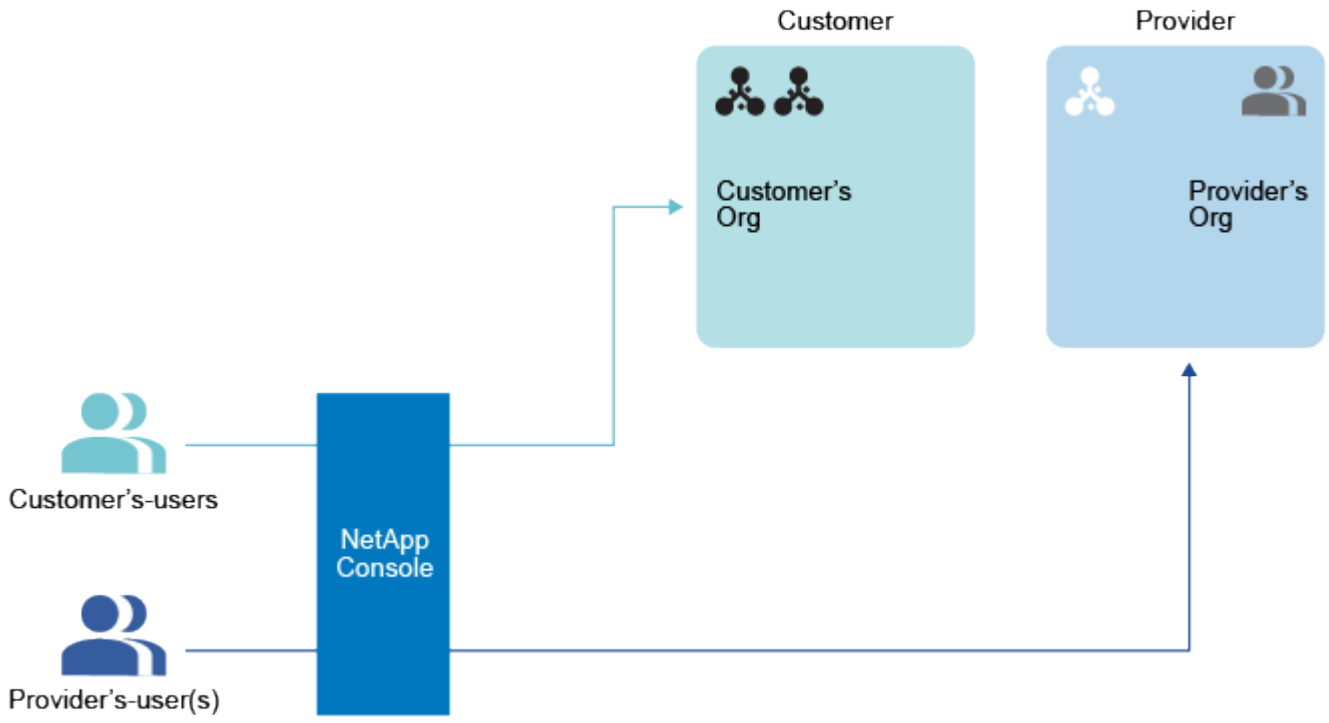
1 Asignar a uno o más usuarios el rol de administrador de asociación

Asigna a uno o varios usuarios, tanto en la organización iniciadora como en la receptora, el rol de Partnership admin para crear y gestionar asociaciones. puedes asignar el rol de Partnership viewer a usuarios que solo necesiten ver asociaciones y no gestionarlas.

2 Comparta el ID de su organización con la organización iniciadora

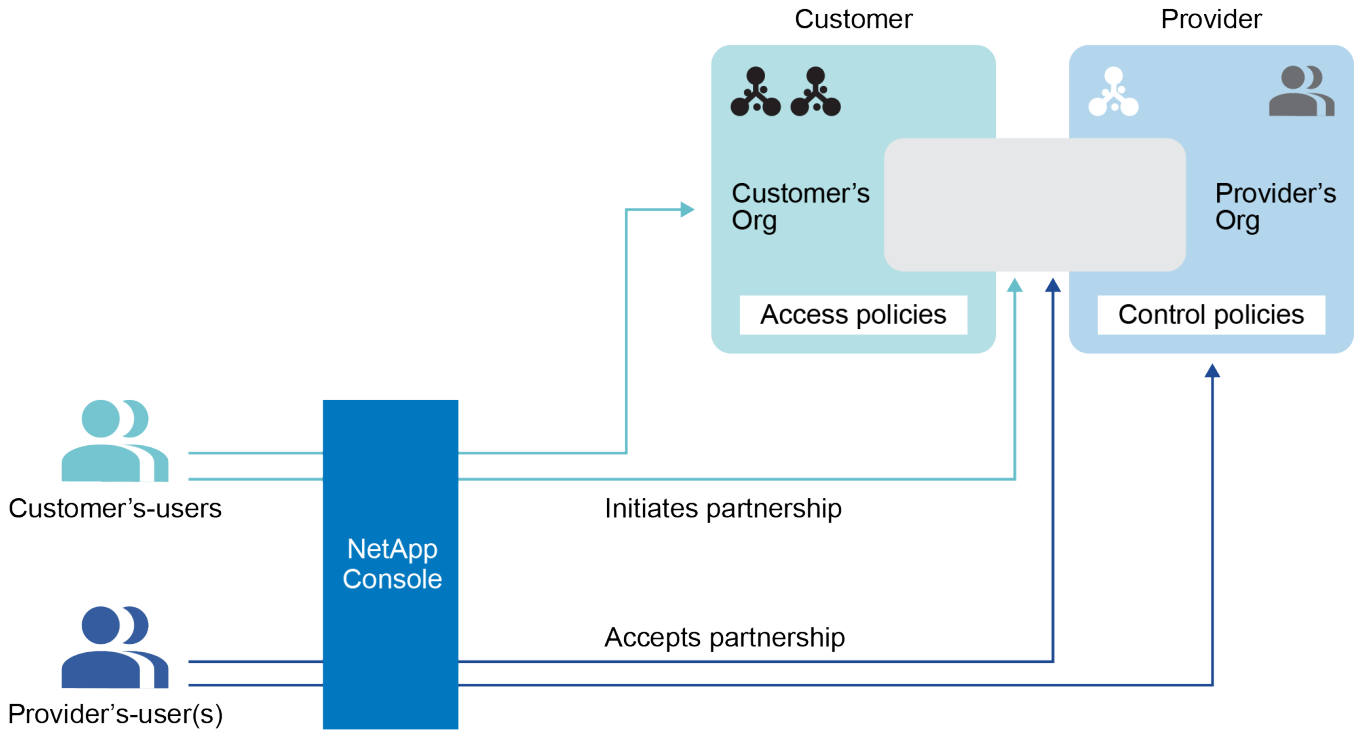
Para iniciar una asociación, el iniciador debe conocer el ID de la organización de destino. Sólo la organización respectiva puede acceder a esta ID de organización. Compártalo directamente con la organización iniciadora fuera de la NetApp Console mediante correo electrónico u otro método.

La organización iniciadora es la organización que concede acceso a sus recursos.



3 Inicie la asociación dentro de la NetApp Console

La organización que inicia la asociación lo hace desde la NetApp Console enviando una solicitud de asociación.



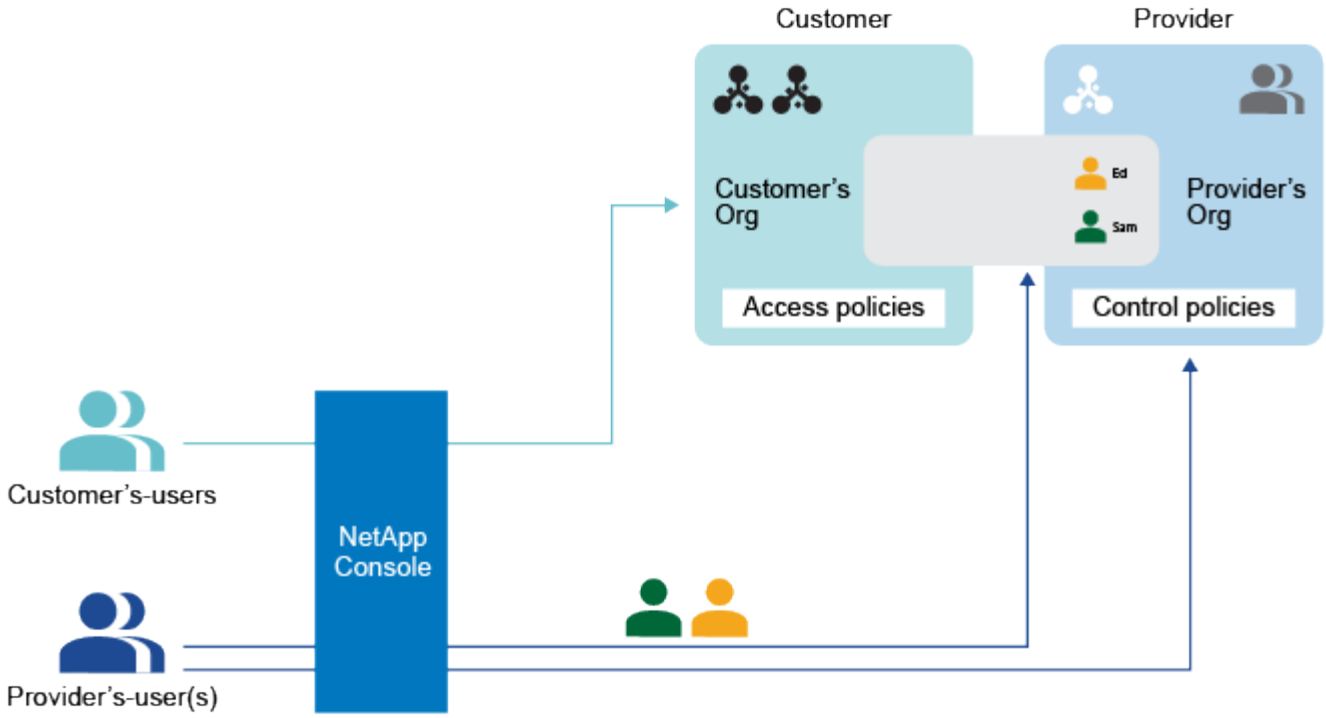
4 Aprobar la asociación

La organización receptora debe aceptar la solicitud.

La organización receptora es la organización a la que se le concede acceso a los recursos.

5 Asignar usuarios a la asociación

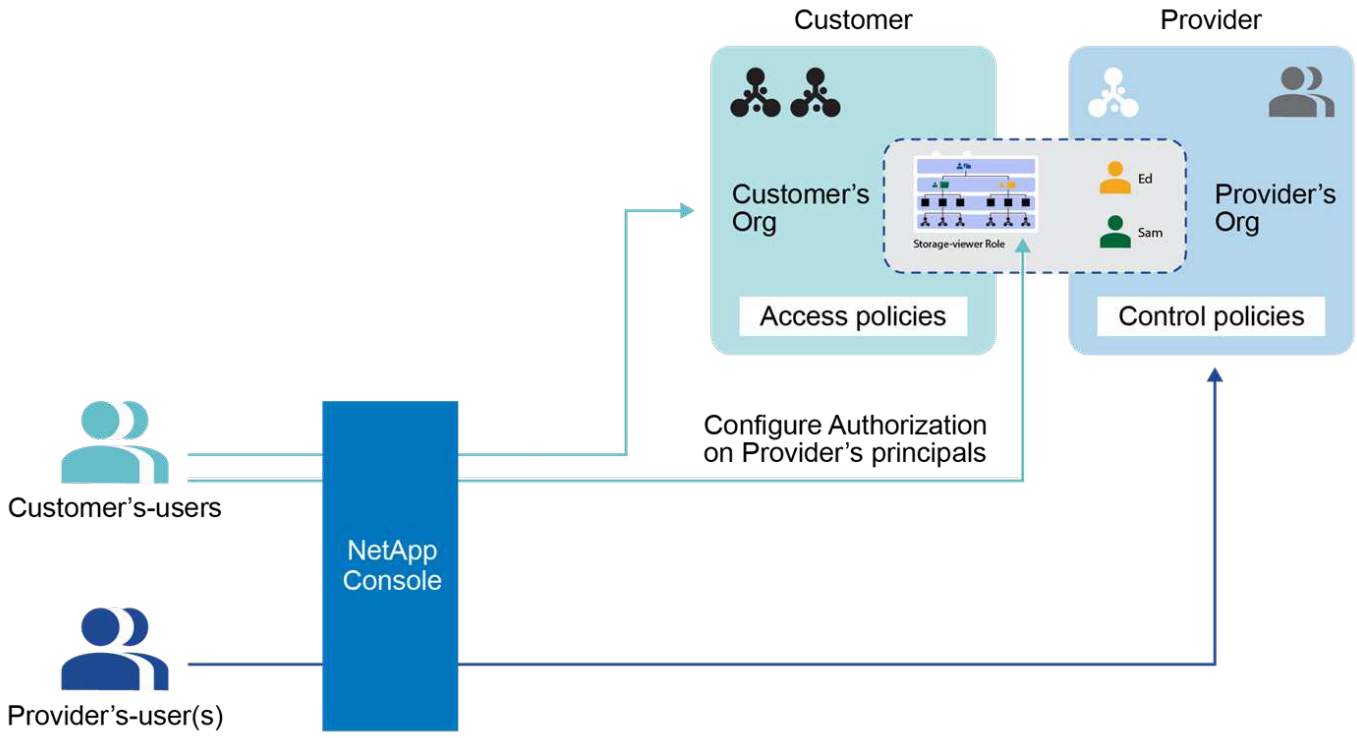
La organización receptora asigna usuarios específicos o cuentas de servicio de su organización a la asociación. La organización iniciadora asigna roles a estos usuarios.



6 Otorgar a los usuarios asignados acceso a los recursos

Si usted es la organización iniciadora, puede otorgar acceso a recursos específicos a los usuarios que fueron asignados a la asociación. Puede revocar el acceso en cualquier momento.

Puede hacerlo asignando roles para proyectos o carpetas específicos dentro de su organización.



Administrar asociaciones en la NetApp Console

Cree asociaciones para establecer conexiones seguras y administradas entre su organización y socios de confianza para la gestión colaborativa de recursos de NetApp .

Las asociaciones le permiten administrar de forma segura los recursos de NetApp a través de los límites con relaciones basadas en roles en la consola. La organización iniciadora concede acceso a sus recursos, mientras que la organización receptora proporciona los usuarios o las cuentas de servicio a los que se les concederá acceso. Las asociaciones se establecen a través de un flujo de trabajo de autoservicio, que brinda a la organización iniciadora control total sobre qué recursos se comparten, qué roles se asignan y la capacidad de incorporar, administrar o revocar el acceso de los socios según sea necesario.

Roles requeridos

El rol de **Administrador de asociación** es necesario para crear y gestionar asociaciones. El **visor de asociaciones** puede ver la página de Asociaciones."Obtenga más información sobre los roles de acceso."

Iniciar una asociación organizacional

Puede solicitar una asociación con otra organización si conoce su ID de organización. La organización receptora aprueba la solicitud antes de que la asociación pueda continuar.

Antes de comenzar, asegúrese de tener el ID de la organización asociada y de que se le haya asignado el rol de **Administrador de asociación**.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione la pestaña **Asociaciones**.
3. Seleccione **Agregar asociación**.
4. En el cuadro de diálogo **Crear asociación**, ingrese el ID de la organización asociada solicitada y seleccione **Agregar**.

   La solicitud de asociación se envía a la organización asociada para su aprobación. Puede ver el estado de la solicitud de asociación en la página **Asociaciones**.

Aprobar una asociación organizacional

Una solicitud de asociación entre una organización y otra debe ser aceptada por la organización receptora antes de que la asociación pueda continuar. Debe tener el rol de **Administrador de asociaciones** para aprobar y administrar asociaciones.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Asociaciones**.
3. Seleccione la pestaña **Asociación recibida**.
4. Navegue hasta la asociación recibida que desea aprobar y seleccione ••• y luego seleccione **Aprobar**.
5. Revise los detalles de la asociación, incluido el nombre y el ID de la organización que solicitó la asociación y seleccione **Siguiente**.
6. Opcional, agregue miembros de la organización a la asociación y seleccione **Aplicar**.

Puede agregar miembros adicionales a través de la página **Asociación** en cualquier momento.

> Cualquier miembro que agregue se volverá visible en la organización del socio, donde el socio puede asignarlos a recursos.

Resultado

La asociación que usted aprobó ahora muestra un estado de **Establecido**. Los usuarios con roles de **Administrador de asociación** o **Visor de asociación** en cualquiera de las organizaciones pueden ver la asociación.

Ver el estado de la asociación

Vea el estado de sus asociaciones.

Rol requerido

Administrador de asociaciones, visor de asociaciones."Obtenga más información sobre los roles de acceso."

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione las **Asociaciones**.
3. Seleccione la pestaña **Asociaciones iniciadas** o **Asociaciones recibidas**.
4. Revise la tabla respectiva que muestra las asociaciones y sus estados.

Deshabilitar una asociación de organización

Debe ser miembro de la organización iniciadora para deshabilitar una asociación. Al deshabilitar una asociación, se revoca inmediatamente el acceso a cualquier recurso de su organización que se haya compartido con la organización asociada.

Rol requerido

Administrador de asociación."Obtenga más información sobre los roles de acceso."

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione las **Asociaciones**.
3. Seleccione la pestaña **Asociaciones iniciadas**.
4. Revise la tabla respectiva que muestra las asociaciones y sus estados.
5. Navegue hasta la asociación iniciada que desea deshabilitar y seleccione ••• y luego seleccione **Deshabilitar**.

Administrar miembros para una organización asociada

Puedes agregar usuarios a una asociación agregándolos a la organización asociada. Después de agregar usuarios, la organización asociada es responsable de asignarles roles para recursos específicos en su organización.

Roles requeridos

El rol de **Administrador de asociación** es necesario para crear y gestionar asociaciones. El **visor de**

asociaciones puede ver la página de Asociaciones."Obtenga más información sobre los roles de acceso."

Puedes eliminar usuarios de una asociación en cualquier momento. Eliminar a un usuario de una asociación revoca inmediatamente su acceso a cualquier recurso en la organización asociada.

Agregar miembros a una asociación

Cuando agrega miembros a una asociación, el **administrador de la asociación** de la organización asociada debe asignarles roles para recursos específicos en su organización antes de que puedan acceder a esos recursos.

Después de agregar miembros a una asociación, los miembros se muestran como miembros en la organización asociada, donde el socio puede asignarlos a los recursos.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Asociaciones**.
3. Seleccione la pestaña **Asociación recibida**.
4. Seleccione el menú de acciones ••• junto a la asociación establecida a la que desea agregar miembros, seleccione **Agregar miembros**.
5. Elija uno o más miembros para agregarlos a la asociación y seleccione **Agregar**.

Eliminar miembros de una asociación

Puedes eliminar miembros de una asociación en cualquier momento. Eliminar a un usuario de una asociación revoca inmediatamente su acceso a cualquier recurso en la organización asociada.

Si desea ajustar el rol que tiene un miembro o los recursos a los que puede acceder, el administrador de la asociación de la organización asociada debe realizar esos cambios.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Asociaciones**.
3. Seleccione la pestaña **Asociación recibida**.
4. Seleccione el menú de acciones ••• junto al miembro que desea eliminar y seleccione **Eliminar asociación**.
5. Confirme la acción seleccionando **Eliminar** en el cuadro de diálogo.

Ver información de roles de un usuario

Puede ver el rol que se le ha asignado a un usuario y los recursos asociados.

No se puede cambiar el rol asociado a un usuario. Si tiene preguntas sobre los recursos o el rol proporcionado, comuníquese con el administrador de la organización asociada.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Asociaciones**.
3. Seleccione la pestaña **Asociación recibida**.

4. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Ver detalles**.
5. En la tabla, expanda la fila correspondiente a la organización, carpeta o proyecto donde desea ver el rol asignado al miembro y seleccione el número en la columna **Rol**.

Proporcionar acceso a recursos a los usuarios asociados

Puede otorgar acceso a los usuarios asociados asignándoles roles específicos para carpetas y proyectos dentro de su organización.

Roles requeridos

Administrador de asociación."Obtenga más información sobre los roles de acceso."

Una organización asociada primero debe agregar miembros a la asociación antes de poder asignarles roles para los recursos de su organización."Aprenda cómo agregar miembros a una asociación."

Comprender los roles de los usuarios asociados

Puede administrar los roles de los miembros de las organizaciones asociadas de la misma manera que lo hace con los suyos propios. Sin embargo, no todos los roles están disponibles para los usuarios asociados. En particular, no puede otorgar a los usuarios socios un rol que permita actualizaciones de software. La actualización del software ONTAP generalmente requiere acceso directo a la red.

Puede asignar los siguientes roles a los usuarios socios:

- "Administrador de la organización"
- "Administrador de carpetas o proyectos"
- "Administración de la federación"
- "Visor de la Federación"
- "Administrador de copias de seguridad y recuperación"
- "Visor de copias de seguridad"
- "Restaurar administrador"
- "Clonar administrador"
- "Administración de recuperación ante desastres"
- "Administrador de conmutación por error de recuperación ante desastres"
- "Administrador de aplicaciones de recuperación ante desastres"
- "Visor de recuperación ante desastres"
- "Analista de soporte de operaciones"
- "Visor de clasificación"

"Obtenga más información sobre los roles predefinidos"

Agregar un rol a un usuario socio

Proporciona acceso a los recursos de su organización agregando un rol a un miembro. Cuando se asigna un rol, se especifica un recurso y un rol. Puede asignar más de un rol a un usuario.

Por ejemplo, si tuviera dos proyectos y quisiera que el mismo usuario tuviera el rol de administrador de respaldo y recuperación para ambos, necesitaría proporcionarle el rol al usuario para cada proyecto. De manera similar, si quisiera proporcionar a un usuario dos roles diferentes para el mismo proyecto, necesitaría asignar cada rol por separado.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Asociaciones**.
3. Seleccione la pestaña **Asociación iniciada**.
4. Seleccione el menú de acciones ••• junto a la asociación establecida que desea ver, seleccione **Ver detalles**.

   La lista **Miembro** muestra los miembros que la organización asociada ha agregado a la asociación.

5. Seleccione el menú de acciones ••• junto al miembro al que desea asignar un rol y seleccione **Agregar un rol**.
6. Para agregar un rol, complete los pasos en el cuadro de diálogo:
   - **Seleccione una organización, carpeta o proyecto**: elija el nivel de su jerarquía de recursos para el cual el miembro debe tener permisos.

     Si selecciona la organización o una carpeta, el miembro tendrá permisos sobre todo lo que resida dentro de la organización o carpeta.

   - **Seleccionar una categoría**: Elija una categoría de rol. "Obtenga más información sobre los roles de acceso" .
   - Seleccionar un **Rol**: elija un rol que proporcione al miembro permisos para los recursos asociados con la organización, carpeta o proyecto que seleccionó.
   - **Agregar rol**: si desea proporcionar acceso a carpetas o proyectos adicionales dentro de su organización, seleccione **Agregar rol**, especifique otra carpeta, proyecto o categoría de rol y luego seleccione una categoría de rol y un rol correspondiente.
7. Seleccione **Agregar nuevos roles**.

Cambiar o eliminar un rol de un usuario socio

Puede cambiar o eliminar un rol que haya asignado a un miembro de una organización asociada.

Pasos

1. Seleccione **Administración > Identidad y acceso**.
2. Seleccione **Asociaciones**.
3. Seleccione la pestaña **Asociación iniciada**.
4. Seleccione el menú de acciones ••• junto a la asociación establecida que desea ver, seleccione **Ver detalles**.

   La lista **Miembro** muestra los miembros que la organización asociada ha agregado a la asociación.

5. Desde la página **Miembros**, navegue hasta un miembro en la tabla, seleccione ••• y luego seleccione **Ver detalles**.
6. En la tabla, expanda la fila correspondiente a la organización, carpeta o proyecto donde desea cambiar el rol asignado al miembro y seleccione **Ver** en la columna **Rol** para ver los roles asignados a este miembro.

7. Puede cambiar un rol existente de un miembro o eliminar un rol.
    a. Para cambiar el rol de un miembro, seleccione **Cambiar** junto al rol que desea cambiar. Sólo puedes cambiar un rol a un rol dentro de la misma categoría de rol. Por ejemplo, puede cambiar de un rol de servicio de datos a otro. Confirmar el cambio.
    b. Para desasignar el rol de un miembro, seleccione junto al rol para eliminar el rol respectivo del miembro.. Se le pedirá que confirme la eliminación.

Trabajar en una organización asociada

Una vez que se le haya asignado un rol en una organización asociada, puede cambiar a esa organización y realizar las acciones que tiene permiso para realizar.

Utilice el menú Organización para alternar entre sus organizaciones y cualquier organización asociada a la que tenga acceso."Obtenga más información sobre cómo cambiar de organizaciones y proyectos."

Podrás ver los recursos que se han compartido contigo en la organización asociada y realizar acciones según el rol que se te haya asignado. Trabaje con el administrador de su asociación para asegurarse de tener el rol adecuado para los recursos a los que necesita acceder.

Supervisar las operaciones de la NetApp Console

Puede supervisar el estado de las operaciones que está realizando la consola para ver si hay algún problema que deba solucionar. Puede ver el estado desde la página de Auditoría, el Centro de notificaciones o recibir notificaciones en su correo electrónico.

La tabla destaca las características de la página Auditoría y del Centro de notificaciones comparándolas.

Centro de notificaciones	Página de auditoría
Muestra el estado de alto nivel de eventos y acciones.	Proporciona detalles de cada evento o acción para una mayor investigación.
Muestra el estado de la sesión de inicio de sesión actual (la información no aparece en el Centro de notificaciones después de cerrar la sesión)	Mantiene el estado del último mes
Muestra solo acciones iniciadas en la interfaz de usuario	Muestra todas las acciones de la interfaz de usuario o las API
Muestra acciones iniciadas por el usuario	Muestra todas las acciones, ya sean iniciadas por el usuario o por el sistema.
Filtrar resultados por importancia	Filtrar por servicio, acción, usuario, estado y más
Proporciona la posibilidad de enviar notificaciones por correo electrónico a los usuarios y a otras personas.	Sin capacidad de correo electrónico

Auditar la actividad del usuario desde la página Auditoría

Utilice la página Auditoría para identificar quién realizó una acción o su estado.

La página Auditoría muestra las acciones que los usuarios completaron para administrar su organización o cuenta. Esto incluye acciones de gestión como asociar usuarios, crear sistemas, crear agentes y más.

También puedes verificar quién agregó un miembro a una organización o que un proyecto se eliminó correctamente.

Pasos

1. Seleccione **Administración > Auditoría**.
2. Utilice los filtros sobre la tabla para cambiar qué acciones se muestran en la tabla.

   Por ejemplo, puede utilizar el filtro **Servicio** para mostrar acciones relacionadas con un servicio específico, o puede utilizar el filtro **Usuario** para mostrar acciones relacionadas con una cuenta de usuario específica.

Descargar registros de auditoría desde la página Auditoría

Puede descargar los registros de auditoría desde la página Auditoría a un archivo CSV. Esto le permite mantener un registro de las acciones que los usuarios realizan en su organización. El archivo CSV incluye todas las columnas del archivo CSV descargado, independientemente de los filtros o las columnas mostradas en la página Auditoría.

Pasos

1. En la página **Auditoría**, seleccione el ícono de descarga en la esquina superior derecha de la tabla.

Supervisar actividades mediante el Centro de notificaciones

Las notificaciones rastrean las operaciones de la consola para confirmar el éxito. Le permiten ver el estado de muchas acciones de la consola que inició durante su sesión de inicio de sesión actual. No todos los servicios de consola reportan información al Centro de notificaciones.

Puede mostrar las notificaciones seleccionando la campana de notificaciones ( ) en la barra de menú. El color de la pequeña burbuja en la campana indica el nivel de gravedad más alto de notificación que está activa. Entonces, si ves una burbuja roja, significa que hay una notificación importante que debes revisar.

También puede configurar la Consola para enviar ciertos tipos de notificaciones por correo electrónico para que pueda estar informado de la actividad importante del sistema incluso cuando no haya iniciado sesión en el sistema. Se pueden enviar correos electrónicos a cualquier usuario que forme parte de su organización o a cualquier otro destinatario que necesite estar al tanto de ciertos tipos de actividad del sistema. Vea cómoEstablecer la configuración de notificaciones por correo electrónico .

Comparación del Centro de notificaciones con las alertas

El Centro de notificaciones le permite ver el estado de las operaciones que ha iniciado y configurar notificaciones de alerta para ciertos tipos de actividades del sistema. Mientras tanto, las alertas le permiten ver problemas o riesgos potenciales en su entorno de almacenamiento ONTAP relacionados con la capacidad, la disponibilidad, el rendimiento, la protección y la seguridad.

"Obtenga más información sobre las alertas de la NetApp Console"

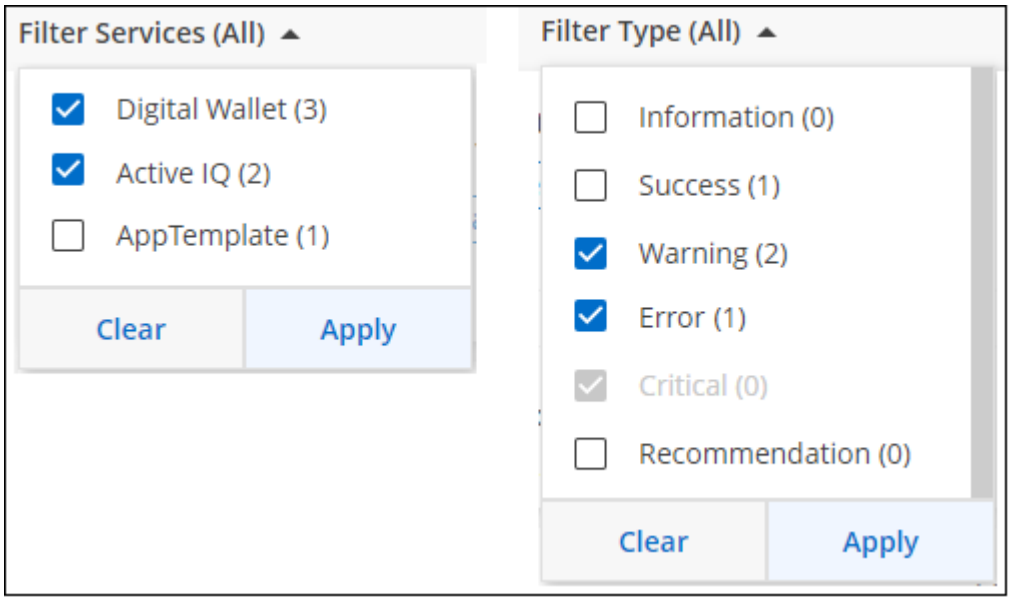
Tipos de notificación

La consola clasifica las notificaciones en las siguientes categorías:

Tipo de notificación	Descripción
Crítico	Se produjo un problema que podría provocar la interrupción del servicio si no se toman medidas correctivas de inmediato.
Error	Una acción o proceso terminó con un fracaso, o podría conducir a un fracaso si no se toman medidas correctivas.
Advertencia	Un problema que debes tener en cuenta para asegurarte de que no alcance una gravedad crítica. Las notificaciones de esta gravedad no provocan interrupciones del servicio y es posible que no se requieran medidas correctivas inmediatas.
Recomendación	Una recomendación del sistema para que usted tome una acción para mejorar el sistema o un determinado servicio; por ejemplo: ahorro de costes, sugerencia de nuevos servicios, configuración de seguridad recomendada, etc.
Información	Un mensaje que proporciona información adicional sobre una acción o proceso.
Éxito	Una acción o proceso completado con éxito.

Filtrar notificaciones

De forma predeterminada, verá todas las notificaciones activas en el Centro de notificaciones. Puedes filtrar las notificaciones que ves para mostrar solo aquellas que son importantes para ti. Puede filtrar por “Servicio” y por “Tipo” de notificación.



Por ejemplo, si desea ver solo notificaciones de "Error" y "Advertencia" para las operaciones de la consola, seleccione esas entradas y verá solo esos tipos de notificaciones.

Descartar notificaciones

Puedes eliminar las notificaciones de la página si ya no necesitas verlas. Puede descartar notificaciones individualmente o todas a la vez.

Para descartar todas las notificaciones, en el Centro de notificaciones, seleccione ⋮ y seleccione **Descartar todo**.

Para descartar notificaciones individuales, pase el cursor sobre la notificación y seleccione **Descartar**.

Establecer la configuración de notificaciones por correo electrónico

Puede enviar tipos específicos de notificaciones por correo electrónico para estar informado sobre la actividad importante del sistema incluso cuando no haya iniciado sesión. Se pueden enviar correos electrónicos a cualquier usuario que forme parte de su organización o cuenta, o a cualquier otro destinatario que necesite estar al tanto de ciertos tipos de actividad del sistema.

- La consola envía notificaciones por correo electrónico para el agente, licencias y suscripciones, NetApp Copy and Sync y NetApp Backup and Recovery.
- No se admite el envío de notificaciones por correo electrónico cuando el agente de la consola está instalado en un sitio sin acceso a Internet.

Los filtros que configure en el Centro de notificaciones no determinan los tipos de notificaciones que recibirá por correo electrónico. De forma predeterminada, cualquier administrador de la organización recibirá correos electrónicos para todas las notificaciones "Críticas" y "Recomendaciones". Estas notificaciones se aplican a todos los servicios: no puede elegir recibir notificaciones solo para ciertos servicios, por ejemplo, agentes o NetApp Backup and Recovery.

Todos los demás usuarios y destinatarios están configurados para no recibir ningún correo electrónico de notificación, por lo que deberá configurar los ajustes de notificación para cualquier usuario adicional.

Debe tener el rol de administrador de la organización para personalizar la configuración de notificaciones.

Pasos

1. Seleccione **Administración > Configuración de notificaciones**.
2. Seleccione **Usuarios de la organización** o **Destinatarios adicionales**.

   La página **Destinatarios adicionales** le permite configurar la Consola para notificar a las personas que son miembros de su organización de la Consola.

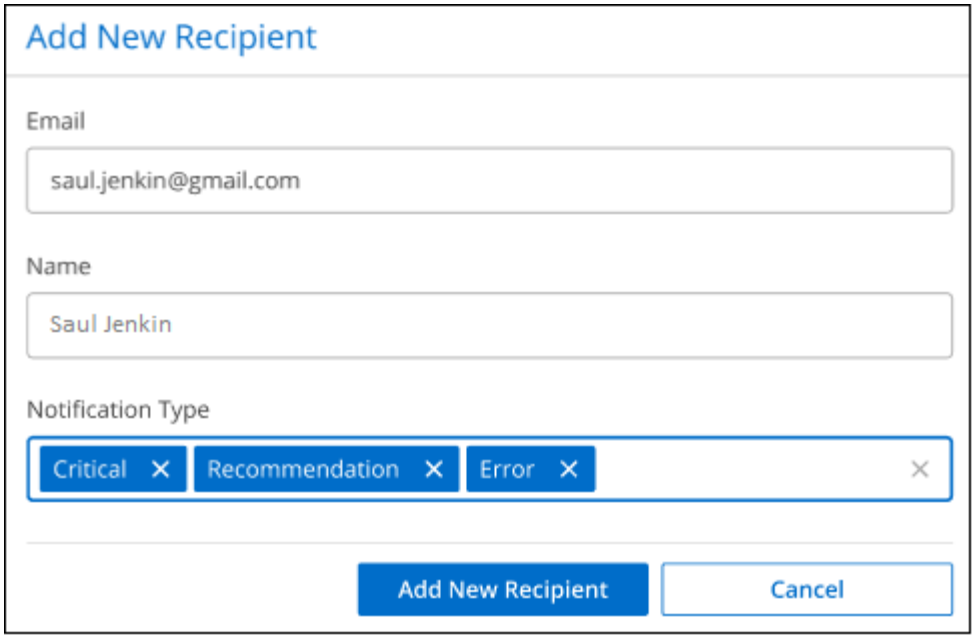
3. Seleccione un usuario o varios usuarios desde la página *Usuarios de la organización* o la página *Destinatarios adicionales* y elija el tipo de notificaciones que se enviarán:
   - Para realizar cambios para un solo usuario, seleccione el menú en la columna Notificaciones para ese usuario, marque los tipos de notificaciones que se enviarán y seleccione **Aplicar**.
   - Para realizar cambios para varios usuarios, marque la casilla de cada usuario, seleccione **Administrar notificaciones por correo electrónico**, marque los tipos de notificaciones que se enviarán y seleccione **Aplicar**.

Agregar destinatarios de correo electrónico adicionales

Los usuarios que aparecen en la página *Usuarios de la organización* se completan automáticamente a partir de los usuarios de su organización o cuenta. Puede agregar direcciones de correo electrónico en la página *Destinatarios adicionales* para otras personas o grupos que no tengan acceso a la Consola, pero que necesiten recibir notificaciones sobre ciertos tipos de alertas y notificaciones.

Pasos

1. Desde la página **Configuración de notificaciones**, seleccione **Agregar nuevos destinatarios**.



2. Ingrese el nombre, la dirección de correo electrónico y seleccione los tipos de notificaciones que recibirá el destinatario y seleccione **Agregar nuevo destinatario**.

Referencia

Consola de mantenimiento del agente

Validación del agente con la consola de mantenimiento

Puede utilizar la consola de mantenimiento del agente de consola para validar la instalación y configuración de un agente de consola.

Acceder a la consola de mantenimiento del agente

Puede acceder a la consola de mantenimiento desde el host del agente de la consola. Navegue al siguiente directorio:

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

Validación del comprobador de configuración

El `config-checker validate` El comando le permite validar la configuración de un agente de consola.

Parámetros

`--services <comma-separated list of services to validate>`**--REQUERIDO--**

Elija uno o más servicios para validar. Los nombres de servicio válidos son:*`PLATFORM` que valida la conectividad de la red a los puntos finales de la consola requeridos.

`--validationTypes <comma-separated list validation types to run>`**--OBLIGATORIO--** Elija entre uno o más tipos de validación para ejecutar. Los tipos de validación válidos son: * `NETWORK` que valida la conectividad de la red a los puntos finales de la consola requeridos.

`--proxy <url>`**--OPCIONAL--**

Especifica la URL del servidor proxy que se utilizará para la validación. Obligatorio si su agente está configurado para utilizar un servidor proxy.

`--certs <paths>`**--OPCIONAL--**

Especifica la ruta a uno o más archivos de certificado que se utilizarán para la validación. Los archivos del certificado deben estar en formato PEM. Separe varias rutas con comas. Este parámetro es necesario si su agente utiliza un certificado personalizado.

Ejemplos de validación del verificador de configuración

Validación básica:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK
```

Validación donde se utiliza un servidor proxy para el agente:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK --proxy http://proxy.company.com:8080
```

Validación donde se utiliza un certificado para el agente:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK --certs /path/to/cert1.pem,/path/to/cert2.pem
```

Ver ayuda para cualquier comando

Para ver la ayuda de cualquier comando, agregue `--help` al mando. Por ejemplo, para ver la ayuda de la `proxy add` Comando, utilice el siguiente comando:

```
./agent-maint-console proxy add --help
```

Comandos de proxy transparentes

Puede utilizar la consola de mantenimiento del agente de consola para configurar un agente de consola para que utilice un servidor proxy transparente.

Acceder a la consola de mantenimiento del agente

Puede acceder a la consola de mantenimiento desde el host del agente de la consola. Navegue al siguiente directorio:

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

Ver ayuda para cualquier comando

Para ver la ayuda de cualquier comando, agregue `--help` al mando. Por ejemplo, para ver la ayuda de la `proxy add` Comando, utilice el siguiente comando:

```
./agent-maint-console proxy add --help
```

obtención de proxy

El `proxy get` El comando muestra información sobre la configuración actual del servidor proxy transparente. Para ver la configuración actual del servidor proxy transparente, utilice el siguiente comando:

Ejemplo de obtención de proxy

Para ver la configuración actual del servidor proxy transparente, utilice el siguiente comando:

```
./agent-maint-console proxy get
```

añadir proxy

El `proxy add` El comando configura el agente para utilizar un servidor proxy transparente.

Parámetros

`-c <certificate file>`

Especifica la ruta al archivo de certificado para el servidor proxy. El archivo del certificado debe estar en formato PEM. Asegúrese de que el archivo del certificado esté en el mismo directorio que el comando o especifique la ruta completa al archivo del certificado.

Ejemplo de adición de proxy

Para agregar un servidor proxy transparente, utilice el siguiente comando, donde `/home/ubuntu/myCA1.pem` es la ruta al archivo de certificado para el servidor proxy. El archivo del certificado debe estar en formato PEM:

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

actualización de proxy

El `proxy update` El comando le permite actualizar el certificado de un proxy transparente.

Parámetros

`-c <certificate file>`Especifica la ruta al archivo de certificado para el servidor proxy. El archivo del certificado debe estar en formato PEM.

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

Ejemplo de actualización de proxy

Para actualizar el certificado de un servidor proxy transparente, utilice el siguiente comando, donde `/home/ubuntu/myCA1.pem` es la ruta al nuevo archivo de certificado para el servidor proxy. El archivo del certificado debe estar en formato PEM:

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

eliminar proxy

El `proxy remove` El comando elimina la configuración del servidor proxy transparente del agente.

Ejemplo de eliminación de proxy

Para eliminar el servidor proxy transparente, utilice el siguiente comando:

```
./agent-maint-console proxy remove
```

Permisos del agente del proveedor de nube y requisitos de red

Resumen de permisos para la NetApp Console

Necesitará proporcionar al agente de consola los permisos adecuados para que pueda realizar operaciones en su entorno de nube. Utilice los enlaces de esta página para acceder rápidamente a los permisos que necesita según su objetivo.

Permisos de AWS

La NetApp Console requiere permisos de AWS para un agente de consola y para servicios individuales.

Agentes de consola

Meta	Descripción	Enlace
Implementar un agente de consola desde la consola Para implementar un agente de consola en AWS, el usuario necesita permisos específicos.	"Configurar permisos de AWS"	Proporcionar permisos para un agente de consola

NetApp Backup and Recovery

Meta	Descripción	Enlace
Realice copias de seguridad de clústeres ONTAP locales en Amazon S3 con NetApp Backup and Recovery	Al activar las copias de seguridad en sus volúmenes ONTAP , NetApp Backup and Recovery le solicita que ingrese una clave de acceso y un secreto para un usuario de IAM que tenga permisos específicos.	"Configurar permisos S3 para copias de seguridad"

Cloud Volumes ONTAP

Meta	Descripción	Enlace
Proporcionar permisos para los nodos de Cloud Volumes ONTAP	Se debe asociar una función de IAM a cada nodo de Cloud Volumes ONTAP en AWS. Lo mismo ocurre con el mediador HA. La opción predeterminada es dejar que la consola cree los roles de IAM para usted, pero puede usar los suyos propios al crear el sistema en la consola.	"Aprenda a configurar usted mismo los roles de IAM"

NetApp Copy and Sync

Meta	Descripción	Enlace
Implementar el agente de datos en AWS	La cuenta de usuario de AWS que utilice para implementar el agente de datos debe tener los permisos necesarios.	"Permisos necesarios para implementar el agente de datos en AWS"
Proporcionar permisos para el agente de datos	Cuando NetApp Copy and Sync implementa el agente de datos, crea una función de IAM para la instancia del agente de datos. Puede implementar el agente de datos utilizando su propio rol de IAM, si lo prefiere.	"Requisitos para utilizar su propio rol de IAM con el agente de datos de AWS"
Habilitar el acceso a AWS para un agente de datos instalado manualmente	Si utiliza el agente de datos con una relación de sincronización que incluye un bucket S3, deberá preparar el host Linux para el acceso a AWS. Cuando instale el agente de datos, deberá proporcionar claves de AWS para un usuario de IAM que tenga acceso programático y permisos específicos.	"Habilitación del acceso a AWS"

FSx para ONTAP

Meta	Descripción	Enlace
Crear y administrar FSx para ONTAP	Para crear o administrar un sistema Amazon FSx for NetApp ONTAP , debe agregar credenciales de AWS a la consola proporcionando el ARN de una función de IAM que le otorga a la consola los permisos necesarios.	"Aprenda a configurar las credenciales de AWS para FSx"

NetApp Cloud Tiering

Meta	Descripción	Enlace
Integración de clústeres ONTAP locales en Amazon S3	Cuando habilita NetApp Cloud Tiering en AWS, ingresa una clave de acceso y una clave secreta. Estas credenciales se pasan al clúster de ONTAP para que ONTAP pueda organizar los datos en niveles en el depósito S3.	"Configurar permisos S3 para niveles"

Permisos de Azure

La consola requiere permisos de Azure para un agente de consola y para servicios individuales.

Agente de consola

Meta	Descripción	Enlace
Implementar un agente de consola desde la consola	Cuando implementa un agente de consola desde la consola, debe usar una cuenta de Azure o una entidad de servicio que tenga permisos para implementar una máquina virtual del agente de consola en Azure.	"Configurar permisos de Azure"
Proporcionar permisos para un agente de consola	Cuando la consola implementa una máquina virtual del agente de consola en Azure, crea un rol personalizado que proporciona los permisos necesarios para administrar recursos y procesos dentro de esa suscripción de Azure. Debe configurar usted mismo el rol personalizado si inicia un agente de consola desde el mercado, si instala manualmente un agente de consola o si"Agregar más credenciales de Azure a un agente de consola" . Mantenga la política actualizada a medida que se agreguen nuevos permisos en versiones posteriores.	"Permisos de Azure para un agente de consola"

NetApp Backup and Recovery

Meta	Descripción	Enlace
Realice una copia de seguridad de Cloud Volumes ONTAP en el almacenamiento de blobs de Azure	Al usar NetApp Backup and Recovery para realizar copias de seguridad de Cloud Volumes ONTAP, debe agregar permisos a un agente de consola en los siguientes escenarios: • Desea utilizar la función "Buscar y restaurar" • Desea utilizar claves de cifrado administradas por el cliente (CMEK)	• "Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Azure Blob Storage con Backup and Recovery"
Realizar copias de seguridad de clústeres de ONTAP locales en el almacenamiento de blobs de Azure	Al usar NetApp Backup and Recovery para realizar copias de seguridad de clústeres ONTAP locales, debe agregar permisos a un agente de consola para usar la funcionalidad "Buscar y restaurar".	"Realice una copia de seguridad de los datos de ONTAP locales en el almacenamiento de blobs de Azure con Backup and Recovery"

Copia y sincronización de NetApp

Meta	Descripción	Enlace
Implementar el agente de datos en Azure	La cuenta de usuario de Azure que utilice para implementar el agente de datos debe tener los permisos necesarios.	"Permisos necesarios para implementar el agente de datos en Azure"

Permisos de Google Cloud

La consola requiere permisos de Google Cloud para un agente de consola y para servicios individuales.

Agentes de consola

Meta	Descripción	Enlace
Implementar un agente de consola desde la consola	El usuario de Google Cloud que implementa un agente de consola desde la consola necesita permisos específicos para implementar un agente de consola en Google Cloud.	"Configurar permisos para crear un agente de consola"
Proporcionar permisos para un agente de consola	La cuenta de servicio de un agente de consola debe tener permisos específicos para las operaciones diarias. Debe asociar la cuenta de servicio con un agente de consola durante la implementación. Mantenga la política actualizada a medida que se agreguen nuevos permisos en versiones posteriores.	"Configurar permisos para un agente de consola"

NetApp Backup and Recovery

Meta	Descripción	Enlace
Realizar copias de seguridad de Cloud Volumes ONTAP en Google Cloud	Al usar NetApp Backup and Recovery para realizar copias de seguridad de Cloud Volumes ONTAP, debe agregar permisos a un agente de consola en los siguientes escenarios: • Desea utilizar la función "Buscar y restaurar" • Desea utilizar claves de cifrado administradas por el cliente (CMEK)	• "Realice una copia de seguridad de los datos de Cloud Volumes ONTAP en Google Cloud Storage con Backup and Recovery" • "Permisos para CMEK"
Realice copias de seguridad de clústeres ONTAP locales en Google Cloud	Al usar NetApp Backup and Recovery para realizar copias de seguridad de clústeres ONTAP locales, debe agregar permisos a un agente de consola para usar la funcionalidad "Buscar y restaurar".	"Realice una copia de seguridad de los datos locales de ONTAP en Google Cloud Storage con Backup and Recovery"

NetApp Copy and Sync

Meta	Descripción	Enlace
Implementar el agente de datos en Google Cloud	Asegúrese de que el usuario de Google Cloud que implementa el agente de datos tenga los permisos necesarios.	"Permisos necesarios para implementar el agente de datos en Google Cloud"

Meta	Descripción	Enlace
Habilitar el acceso a Google Cloud para un agente de datos instalado manualmente	Si planea utilizar el agente de datos con una relación de sincronización que incluye un depósito de Google Cloud Storage, entonces debe preparar el host Linux para el acceso a Google Cloud. Cuando instale el agente de datos, deberá proporcionar una clave para una cuenta de servicio que tenga permisos específicos.	"Habilitar el acceso a Google Cloud"

Permisos de StorageGRID

La consola requiere permisos de StorageGRID para dos servicios.

NetApp Backup and Recovery

Meta	Descripción	Enlace
Realice copias de seguridad de clústeres ONTAP locales en StorageGRID	Cuando prepara StorageGRID como destino de respaldo para clústeres de ONTAP , NetApp Backup and Recovery le solicita que ingrese una clave de acceso y un secreto para un usuario de IAM que tenga permisos específicos.	"Prepare StorageGRID como su destino de respaldo"

NetApp Cloud Tiering

Meta	Descripción	Enlace
Integración de clústeres ONTAP locales en StorageGRID	Cuando configura NetApp Cloud Tiering en StorageGRID, debe proporcionar a Cloud Tiering una clave de acceso S3 y una clave secreta. La organización en niveles de la nube utiliza las claves para acceder a sus buckets.	"Preparar la organización en niveles para StorageGRID"

Permisos del agente de AWS y reglas de seguridad

Permisos de AWS para el agente de consola

Cuando la NetApp Console inicia un agente de consola en AWS, adjunta una política al agente que le proporciona permisos para administrar recursos y procesos dentro de esa cuenta de AWS. El agente usa los permisos para realizar llamadas API a varios servicios de AWS, incluidos EC2, S3, CloudFormation, IAM, el Servicio de administración de claves (KMS) y más.

Políticas de IAM

Las políticas de IAM disponibles a continuación proporcionan los permisos que un agente de consola necesita para administrar recursos y procesos dentro de su entorno de nube pública en función de su región de AWS.

Tenga en cuenta lo siguiente:

- Si crea un agente de consola en una región estándar de AWS directamente desde la consola, esta aplicará automáticamente las políticas al agente.
- Debe configurar las políticas usted mismo si implementa el agente desde AWS Marketplace, si instala

manualmente el agente en un host Linux o si desea agregar credenciales de AWS adicionales a la consola.

- En cualquier caso, debe asegurarse de que las políticas estén actualizadas a medida que se agreguen nuevos permisos en versiones posteriores. Si se requieren nuevos permisos, se enumerarán en las notas de la versión.
- Si es necesario, puede restringir las políticas de IAM mediante el IAM `Condition` elemento. "Documentación de AWS: Elemento de condición"
- Para ver instrucciones paso a paso sobre cómo utilizar estas políticas, consulte las siguientes páginas:
  - "Configurar permisos para una implementación de AWS Marketplace"
  - "Configurar permisos para implementaciones locales"
  - "Configurar permisos para el modo restringido"

Seleccione su región para ver las políticas requeridas:

Regiones estándar

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.

Política #1

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:CreatePlacementGroup",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateRoute",
        "ec2:DescribeVpcs",
        "ec2:ReplaceRoute",
```

```
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteRoute",
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:ModifyVolume",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "cloudformation:DeleteStack",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:ListInstanceProfiles",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteInstanceProfile",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "sts:DecodeAuthorizationMessage",
        "sts:AssumeRole",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutObject",
        "s3:ListAllMyBuckets",
        "s3:GetObject",
```

```
        "s3:GetEncryptionConfiguration",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "fsx:Describe*",
        "fsx:List*",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "cvoServicePolicy"
    },
    {
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartitions"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
```

```
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
            "s3:GetBucketAcl",
            "s3:PutBucketPublicAccessBlock",
            "s3:GetObject",
            "s3:PutEncryptionConfiguration",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:ListBucketMultipartUploads",
            "s3:PutObject",
            "s3:PutBucketAcl",
            "s3:AbortMultipartUpload",
            "s3:ListMultipartUploadParts",
            "s3:DeleteBucket",
            "s3:GetObjectVersionTagging",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectRetention",
            "s3:GetObjectTagging",
            "s3:GetObjectVersion",
            "s3:PutObjectVersionTagging",
            "s3:PutObjectRetention",
            "s3:DeleteObjectTagging",
            "s3:DeleteObjectVersionTagging",
            "s3:GetBucketObjectLockConfiguration",
            "s3:GetBucketVersioning",
            "s3:PutBucketObjectLockConfiguration",
            "s3:PutBucketVersioning",
            "s3:BypassGovernanceRetention",
            "s3:PutBucketPolicy",
            "s3:PutBucketOwnershipControls"
        ],
        "Resource": [
            "arn:aws:s3:::netapp-backup-*"
        ],
        "Effect": "Allow",
        "Sid": "backupS3Policy"
    },
    {
        "Action": [
            "s3:CreateBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
```

```
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:DeleteBucket"
      ],
      "Resource": [
        "arn:aws:s3:::fabric-pool*"
      ],
      "Effect": "Allow",
      "Sid": "fabricPoolS3Policy"
    },
    {
      "Action": [
        "ec2:DescribeRegions"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "fabricPoolPolicy"
    },
    {
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/netapp-adc-manager": "*"
        }
      },
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Effect": "Allow"
    },
    {
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
```

```
            "ec2:AttachVolume",
            "ec2:DetachVolume",
            "ec2:StopInstances",
            "ec2:DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
            "ec2:DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

Política #2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "tagServicePolicy"
    }
  ]
}
```

Regiones de GovCloud (EE. UU.)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListInstanceProfiles",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "ec2:ModifyVolumeAttribute",
        "sts:DecodeAuthorizationMessage",
        "ec2:DescribeImages",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstances",
        "iam:PassRole",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:DeleteVolume",
        "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:CreateSnapshot",
        "ec2:DeleteSnapshot",
```

```
        "ec2:DescribeSnapshots",
        "ec2:StopInstances",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
```

```
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource": [
        "arn:aws-us-gov:s3:::fabric-pool*"
      ]
    },
    {
      "Sid": "backupPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource": [
        "arn:aws-us-gov:s3:::netapp-backup-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws-us-gov:ec2:*:*:instance/*"
      ]
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "arn:aws-us-gov:ec2:*:*:volume/*"
      ]
    }
  ]
}
```

Regiones secretas

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
```

```
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso-b:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

```
        ],
        "Condition": {
          "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
          }
        },
        "Resource": [
          "arn:aws-iso-b:ec2:*:*:instance/*"
        ]
      },
      {
        "Effect": "Allow",
        "Action": [
          "ec2:AttachVolume",
          "ec2:DetachVolume"
        ],
        "Resource": [
          "arn:aws-iso-b:ec2:*:*:volume/*"
        ]
      }
    ]
}
```

Regiones de alto secreto

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
```

```
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

```
        ],
        "Condition": {
          "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
          }
        },
        "Resource": [
          "arn:aws-iso:ec2:*:*:instance/*"
        ]
      },
      {
        "Effect": "Allow",
        "Action": [
          "ec2:AttachVolume",
          "ec2:DetachVolume"
        ],
        "Resource": [
          "arn:aws-iso:ec2:*:*:volume/*"
        ]
      }
    ]
}
```

Cómo se utilizan los permisos de AWS

Las siguientes secciones describen cómo se utilizan los permisos para cada servicio de datos o administración de la NetApp Console . Esta información puede ser útil si sus políticas corporativas establecen que los permisos solo se otorgan cuando es necesario.

Amazon FSx para ONTAP

El agente de la consola realiza las siguientes solicitudes de API para administrar un sistema de archivos de Amazon FSx para ONTAP :

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CrearEtiquetas
- ec2:DescribeVolúmenes
- ec2:DescribeSecurityGroups
- ec2: Describir interfaces de red
- ec2:DescribeSubnets

- ec2:DescribeVpcs
- ec2:DescribeDhcpOptions
- ec2:DescribeSnapshots
- ec2:DescribeKeyPairs
- ec2:DescribirRegiones
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribeVolumesModifications
- ec2:DescribirGruposDeUbicación
- kms:CrearConcesión
- kms:ListAliases
- fsx:Describir*
- fsx:Lista*

Descubrimiento de buckets de Amazon S3

El agente de la consola realiza la siguiente solicitud de API para descubrir buckets de Amazon S3:

s3:Obtener configuración de cifrado

NetApp Backup and Recovery

El agente realiza las siguientes solicitudes de API para administrar copias de seguridad en Amazon S3:

- s3: Obtener ubicación del depósito
- s3: Listar todos mis cubos
- s3:ListBucket
- s3:CrearCubo
- s3:Obtener configuración del ciclo de vida
- s3:Configuración del ciclo de vida de PutLifecycle
- s3:Etiquetado de cubo de colocación
- s3:ListBucketVersions
- s3:ObtenerAcl del depósito
- s3:PonerCuboBloqueDeAccesoPúblico
- s3:Obtener objeto
- ec2:DescribeVpcEndpoints
- kms:ListAliases
- s3:PonerConfiguraciónDeCifrado

El agente realiza las siguientes solicitudes de API cuando utiliza el método de búsqueda y restauración para restaurar volúmenes y archivos:

- s3:CrearCubo
- s3:EliminarObjeto
- s3:EliminarVersiónDeObjeto
- s3:ObtenerAcl del depósito
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PonerObjeto
- s3:PonerCuboAcl
- s3:Configuración del ciclo de vida de PutLifecycle
- s3:PonerCuboBloqueDeAccesoPúblico
- s3:AbortarCargaMultiparte
- s3:ListaMultiparteSubirPartes

El agente realiza las siguientes solicitudes de API cuando utiliza DataLock y NetApp Ransomware Resilience para sus copias de seguridad de volumen:

- s3: Obtener etiquetado de versión de objeto
- s3:Configuración de bloqueo de objeto de depósito
- s3:ObtenerAcl de versión de objeto
- s3:Etiquetado de objetos de colocación
- s3:EliminarObjeto
- s3:EliminarEtiquetadoDeObjeto
- s3:ObtenerRetenciónDeObjeto
- s3: Eliminar etiquetado de versión de objeto
- s3:PonerObjeto
- s3:Obtener objeto
- s3:Configuración de bloqueo de objeto PutBucket
- s3:Obtener configuración del ciclo de vida
- s3:ListarCuboPorEtiquetas
- s3: Obtener etiquetado de cubo
- s3:EliminarVersiónDeObjeto
- s3:ListBucketVersions
- s3:ListBucket
- s3:Etiquetado de cubo de colocación
- s3:Obtener etiquetado de objeto
- s3:Versión de PutBucket

- s3:Etiquetado de versión de objeto de colocación
- s3: Obtener versiones de Bucket
- s3:ObtenerAcl del depósito
- s3: Retención de gobernanza de bypass
- s3:PonerRetenciónDeObjeto
- s3: Obtener ubicación del depósito
- s3:ObtenerVersiónDeObjeto

El agente realiza las siguientes solicitudes de API si utiliza una cuenta de AWS diferente para sus copias de seguridad de Cloud Volumes ONTAP que la que utiliza para los volúmenes de origen:

- s3:Política de depósito de colocación
- s3: Controles de propiedad del depósito de colocación

Permisos heredados para Copia de seguridad y recuperación

Solo necesitas los siguientes permisos si habilitaste las funciones de indexación heredadas antes del lanzamiento de la versión 2 de indexación:

- kms:Lista*
- kms:Describir*
- athena:IniciarEjecuciónDeConsulta
- atenea:ObtenerResultadosDeConsulta
- athena:ObtenerEjecuciónDeConsulta
- athena:DetenerEjecuciónDeConsulta
- pegamento:CrearBaseDeDatos
- pegamento:CrearTabla
- pegamento:LoteEliminarPartición

Clasificación

El agente realiza las siguientes solicitudes de API para implementar NetApp Data Classification:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:EjecutarInstancias
- ec2:Terminar instancias
- ec2:CrearEtiquetas
- ec2:CrearVolumen
- ec2:AdjuntarVolumen
- ec2:CrearGrupoDeSeguridad
- ec2:EliminarGrupoDeSeguridad
- ec2:DescribeSecurityGroups

- ec2:CrearInterfazDeRed
- ec2: Describir interfaces de red
- ec2:EliminarInterfazDeRed
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:CrearInstantánea
- ec2:DescribirRegiones
- formación de nubes:CreateStack
- formación de nubes:Eliminar pila
- formación de nubes: DescribeStacks
- formación de nubes: DescribeStackEvents
- iam:AñadirRolAlPerfilDeInstancia
- ec2:AsociarPerfilDeInstanciaSoy
- ec2:DescribeIamInstanceProfileAssociations

El agente realiza las siguientes solicitudes de API para escanear los depósitos S3 cuando utiliza la NetApp Data Classification:

- iam:AñadirRolAlPerfilDeInstancia
- ec2:AsociarPerfilDeInstanciaSoy
- ec2:DescribeIamInstanceProfileAssociations
- s3: Obtener etiquetado de cubo
- s3: Obtener ubicación del depósito
- s3: Listar todos mis cubos
- s3:ListBucket
- s3: Obtener estado de la política del depósito
- s3: Obtener política de depósito
- s3:ObtenerAcl del depósito
- s3:Obtener objeto
- soy:ObtenerRole
- s3:EliminarObjeto
- s3:EliminarVersiónDeObjeto
- s3:PonerObjeto
- sts:Asumir rol

Cloud Volumes ONTAP

El agente realiza las siguientes solicitudes de API para implementar y administrar Cloud Volumes ONTAP en AWS.

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Crear y administrar roles de IAM y perfiles de instancia para instancias de Cloud Volumes ONTAP	iam:ListInstanceProfiles	Sí	Sí	No
	soy:CreateRole	Sí	No	No
	iam:EliminarRole	No	Sí	Sí
	soy:PolíticaDeRolDePut	Sí	No	No
	iam:CreateInstanceProfile	Sí	No	No
	iam:DeleteRolePolicy	No	Sí	Sí
	iam:AñadirRolAlPerfilDeInstancia	Sí	No	No
	iam:EliminarRolDePerfilDeInstancia	No	Sí	Sí
	iam:EliminarPerfilDeInstancia	No	Sí	Sí
	yo soy:PassRole	Sí	No	No
	ec2:AsociarPerfilDeInstanciaSoy	Sí	Sí	No
	ec2:DescribeIamInstanceProfileAssociations	Sí	Sí	No
	ec2: Desasociar perfil de instancia de Iam	No	Sí	No
Decodificar mensajes de estado de autorización	sts:Decodificar mensaje de autorización	Sí	Sí	No
Describe las imágenes específicas (AMI) disponibles para la cuenta	ec2:DescribeImages	Sí	Sí	No
Describe las tablas de rutas en una VPC (requerida solo para pares de alta disponibilidad)	ec2:DescribeRouteTables	Sí	No	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Detener, iniciar y supervisar instancias	ec2:Instancias de inicio	Sí	Sí	No
	ec2:Detener instancias	Sí	Sí	No
	ec2:DescribeInstances	Sí	Sí	No
	ec2:DescribeInstanceStatus	Sí	Sí	No
	ec2:EjecutarInstancias	Sí	No	No
	ec2:Terminar instancias	No	No	Sí
	ec2:ModificarAtributoDeInstancia	No	Sí	No
Verifique que la red mejorada esté habilitada para los tipos de instancias compatibles	ec2:DescribeInstanceAttribute	No	Sí	No
Etiquete los recursos con las etiquetas "WorkingEnvironment" y "WorkingEnvironmentId", que se utilizan para el mantenimiento y la asignación de costos.	ec2:CrearEtiquetas	Sí	Sí	No
Administrar volúmenes EBS que Cloud Volumes ONTAP utiliza como almacenamiento de backend	ec2:CrearVolumen	Sí	Sí	No
	ec2:DescribeVolúmenes	Sí	Sí	Sí
	ec2:ModificarAtributoDeVolumen	No	Sí	Sí
	ec2:AdjuntarVolumen	Sí	Sí	No
	ec2:EliminarVolumen	No	Sí	Sí
	ec2:Separar volumen	No	Sí	Sí

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Crear y administrar grupos de seguridad para Cloud Volumes ONTAP	ec2:CrearGrupoDeSeguridad	Sí	No	No
	ec2:EliminarGrupoDeSeguridad	No	Sí	Sí
	ec2:DescribeSecurityGroups	Sí	Sí	Sí
	ec2:Revocar salida del grupo de seguridad	Sí	No	No
	ec2:AutorizarSalidaGrupoSeguridad	Sí	No	No
	ec2:AutorizarIngresoDeGrupoDeSeguridad	Sí	No	No
	ec2: Revocar entrada de grupo de seguridad	Sí	Sí	No
Cree y administre interfaces de red para Cloud Volumes ONTAP en la subred de destino	ec2:CrearInterfazDeRed	Sí	No	No
	ec2: Describir interfaces de red	Sí	Sí	No
	ec2:EliminarInterfazDeRed	No	Sí	Sí
	ec2:ModificarAtributoDeInterfazDeRed	No	Sí	No
Obtenga la lista de subredes de destino y grupos de seguridad	ec2:DescribeSubnets	Sí	Sí	No
	ec2:DescribeVpcs	Sí	Sí	No
Obtenga servidores DNS y el nombre de dominio predeterminado para las instancias de Cloud Volumes ONTAP	ec2:DescribeDhcpOptions	Sí	No	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Tomar instantáneas de volúmenes EBS para Cloud Volumes ONTAP	ec2:CrearInstantánea	Sí	Sí	No
	ec2:Eliminar instantánea	No	Sí	Sí
	ec2:DescribeSnapshots	No	Sí	No
Captura la consola Cloud Volumes ONTAP , que está adjunta a los mensajes de AutoSupport	ec2:ObtenerSalidaDeLaConsola	Sí	Sí	No
Obtenga la lista de pares de claves disponibles	ec2:DescribeKeyPairs	Sí	No	No
Obtenga la lista de regiones de AWS disponibles	ec2:DescribirRegiones	Sí	Sí	No
Administrar etiquetas para recursos asociados con instancias de Cloud Volumes ONTAP	ec2:EliminarEtiquetas	No	Sí	Sí
	ec2:DescribeTags	No	Sí	No
Crear y administrar pilas para plantillas de AWS CloudFormation	formación de nubes:CreateStack	Sí	No	No
	formación de nubes:Eliminar pila	Sí	No	No
	formación de nubes: DescribeStacks	Sí	Sí	No
	formación de nubes: DescribeStackEvents	Sí	No	No
	formación de nubes: Validar plantilla	Sí	No	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Cree y administre un bucket S3 que un sistema Cloud Volumes ONTAP utiliza como nivel de capacidad para la clasificación de datos	s3:CrearCubo	Sí	Sí	No
	s3:Eliminar depósito	No	Sí	Sí
	s3:Obtener configuración del ciclo de vida	No	Sí	No
	s3:Configuración del ciclo de vida de PutLifecycle	No	Sí	No
	s3:Etiquetado de cubo de colocación	No	Sí	No
	s3:ListBucketVersions	No	Sí	No
	s3: Obtener estado de la política del depósito	No	Sí	No
	s3:ObtenerBloqueDeAccesoPúblicoDeBucket	No	Sí	No
	s3:ObtenerAcl del depósito	No	Sí	No
	s3: Obtener política de depósito	No	Sí	No
	s3:PonerCuboBloqueDeAccesoPúblico	No	Sí	No
	s3: Obtener etiquetado de cubo	No	Sí	No
	s3: Obtener ubicación del depósito	No	Sí	No
	s3: Listar todos mis cubos	No	No	No
	s3:ListBucket	No	Sí	No
Habilite el cifrado de datos de Cloud Volumes ONTAP mediante el Servicio de administración de claves de AWS (KMS)	kms:ReEncrypt*	Sí	No	No
	kms:CrearConcesión	Sí	Sí	No
	kms:GenerarClaveDeDatosSinTextoSimple	Sí	Sí	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Cree y administre un grupo de ubicación distribuida de AWS para dos nodos de alta disponibilidad y el mediador en una única zona de disponibilidad de AWS	ec2:CrearGrupoDeUbicación	Sí	No	No
	ec2:EliminarGrupoDeUbicación	No	Sí	Sí
Crear informes	fsx:Describir*	No	Sí	No
	fsx:Lista*	No	Sí	No
Cree y administre agregados que admitan la función de volúmenes elásticos de Amazon EBS	ec2:DescribeVolumesModifications	No	Sí	No
	ec2:ModificarVolumen	No	Sí	No
Verifique si la zona de disponibilidad es una zona local de AWS y valide que todos los parámetros de implementación sean compatibles	ec2:Describir zonas de disponibilidad	Sí	No	Sí

Registro de cambios

A medida que se agreguen y eliminen permisos, los indicaremos en las secciones siguientes.

11 de noviembre de 2025

Los siguientes permisos ya no son necesarios para NetApp Backup and Recovery a menos que utilice la indexación heredada. Estos permisos se han eliminado de las políticas de esta página:

- kms:Lista*
- kms:Describir*
- athena:IniciarEjecuciónDeConsulta
- atenea:ObtenerResultadosDeConsulta
- athena:ObtenerEjecuciónDeConsulta
- athena:DetenerEjecuciónDeConsulta
- pegamento:CrearBaseDeDatos
- pegamento:CrearTabla
- pegamento:LoteEliminarPartición

9 de septiembre de 2024

Se eliminaron los permisos de la política n.° 2 para las regiones estándar porque la NetApp Console ya no admite el almacenamiento en caché perimetral de NetApp ni el descubrimiento y la administración de clústeres de Kubernetes.

Ver los permisos que se eliminaron de la política

```
{
    "Action": [
        "ec2:DescribeRegions",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "K8sServicePolicy"
},
{
    "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "GFCservicePolicy"
},
{
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/GFCInstance": "*"
        }
    },
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Effect": "Allow"
}
```

9 de mayo de 2024

Ahora se requiere el siguiente permiso para Cloud Volumes ONTAP:

ec2:Describir zonas de disponibilidad

6 de junio de 2023

Ahora se requiere el siguiente permiso para Cloud Volumes ONTAP:

kms:GenerarClaveDeDatosSinTextoSimple

14 de febrero de 2023

Ahora se requiere el siguiente permiso para NetApp Cloud Tiering:

ec2:DescribeVpcEndpoints

Reglas del grupo de seguridad del agente de consola en AWS

El grupo de seguridad de AWS para el agente requiere reglas entrantes y salientes. La NetApp Console crea automáticamente este grupo de seguridad cuando usted crea un agente de consola desde la consola. Debe configurar este grupo de seguridad para todas las demás opciones de instalación.

Reglas de entrada

Protocolo	Puerto	Objetivo
SSH	22	Proporciona acceso SSH al host del agente
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 a la interfaz de usuario local y conexiones desde la instancia de NetApp Data Classification
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet. Debe abrir este puerto manualmente después de la implementación.

Reglas de salida

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

Reglas básicas de salida

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

Protocolo	Puerto	Objetivo
Todo TCP	Todo	Todo el tráfico saliente
Todos los UDP	Todo	Todo el tráfico saliente

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede usar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

Servicio	Protocolo	Puerto	Destino	Objetivo
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres ONTAP e Internet saliente	Llamadas API a AWS, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp
Llamadas API	TCP	3000	Mediador de HA de ONTAP	Comunicación con el mediador de ONTAP HA
	TCP	8080	Clasificación de datos	Sonda a la instancia de clasificación de datos durante la implementación
DNS	UDP	53	DNS	Utilizado para la resolución de DNS por la consola

Permisos de Azure y reglas de seguridad requeridas

Permisos de Azure para el agente de consola

Cuando la NetApp Console inicia un agente de consola en Azure, adjunta un rol personalizado a la máquina virtual que proporciona al agente permisos para administrar recursos y procesos dentro de esa suscripción de Azure. El agente usa los permisos para realizar llamadas API a varios servicios de Azure.

Si necesita o no crear este rol personalizado para el agente depende de cómo lo haya implementado.

Implementación desde la NetApp Console

Cuando se usa la consola para implementar la máquina virtual del agente en Azure, se 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. Los permisos del rol se mantienen actualizados cuando se actualiza el agente. No es necesario crear este rol para el agente ni administrar actualizaciones.

Implementación manual o desde Azure Marketplace

Cuando implementa el agente desde Azure Marketplace o si instala manualmente el agente en un host Linux, deberá configurar usted mismo el rol personalizado y mantener sus permisos con cualquier cambio.

Deberá asegurarse de que el rol esté actualizado a medida que se agreguen nuevos permisos en versiones posteriores. Si se requieren nuevos permisos, se enumerarán en las notas de la versión.

- Para ver instrucciones paso a paso sobre cómo utilizar estas políticas, consulte las siguientes páginas:
  - "Configurar permisos para una implementación de Azure Marketplace"
  - "Configurar permisos para implementaciones locales"
  - "Configurar permisos para el modo restringido"

```
{
  "Name": "Console Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/write",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/write",
    "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.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",
    "Microsoft.Storage/storageAccounts/listkeys/action",
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Storage/storageAccounts/blobServices/containers/read",
    "Microsoft.Storage/storageAccounts/listAccountSas/action",
    "Microsoft.Storage/usages/read",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/read",
    "Microsoft.Compute/availabilitySets/write",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
    "Microsoft.Network/loadBalancers/read",
    "Microsoft.Network/loadBalancers/write",
    "Microsoft.Network/loadBalancers/delete",
    "Microsoft.Network/loadBalancers/backendAddressPools/read",
    "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
    "Microsoft.Network/loadBalancers/loadBalancingRules/read",
    "Microsoft.Network/loadBalancers/probes/read",
    "Microsoft.Network/loadBalancers/probes/join/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Network/routeTables/join/action",
    "Microsoft.NetApp/netAppAccounts/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
    "Microsoft.Storage/storageAccounts/privateEndpointConnections/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/write",
    "Microsoft.Network/privateEndpoints/read",
```

```
    "Microsoft.Network/privateDnsZones/write",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/privateDnsZones/A/write",
    "Microsoft.Network/privateDnsZones/read",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/delete",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Compute/diskEncryptionSets/read",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Network/privateEndpoints/delete",
    "Microsoft.Compute/availabilitySets/delete",
    "Microsoft.KeyVault/vaults/read",
    "Microsoft.KeyVault/vaults/accessPolicies/write",
    "Microsoft.Compute/diskEncryptionSets/write",
    "Microsoft.KeyVault/vaults/deploy/action",
    "Microsoft.Compute/diskEncryptionSets/delete",
    "Microsoft.Resources/tags/read",
    "Microsoft.Resources/tags/write",
    "Microsoft.Resources/tags/delete",
    "Microsoft.Network/applicationSecurityGroups/write",
    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/applicationSecurityGroups/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Synapse/workspaces/write",
    "Microsoft.Synapse/workspaces/read",
    "Microsoft.Synapse/workspaces/delete",
    "Microsoft.Synapse/register/action",
    "Microsoft.Synapse/checkNameAvailability/action",
    "Microsoft.Synapse/workspaces/operationStatuses/read",
    "Microsoft.Synapse/workspaces/firewallRules/read",
    "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",
    "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
```

```
            "Microsoft.Compute/images/write",
            "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
            "Microsoft.Compute/virtualMachineScaleSets/write",
            "Microsoft.Compute/virtualMachineScaleSets/read",
            "Microsoft.Compute/virtualMachineScaleSets/delete"
        ],
        "NotActions": [],
        "AssignableScopes": [],
        "Description": "Console Permissions",
        "IsCustom": "true"
    }
```

Cómo se utilizan los permisos de Azure

Las siguientes secciones describen cómo se utilizan los permisos para cada sistema de almacenamiento y servicio de datos de NetApp . Esta información puede ser útil si sus políticas corporativas establecen que los permisos solo se otorgan cuando es necesario.

Azure NetApp Files

El agente realiza las siguientes solicitudes de API cuando se usa NetApp Data Classification para escanear datos de Azure NetApp Files :

- Microsoft. NetApp/netAppAccounts/read
- Microsoft. NetApp/netAppAccounts/capacityPools/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

Las siguientes secciones describen cómo se utilizan los permisos para NetApp Backup and Recovery.

Permisos mínimos de NetApp Backup and Recovery

El agente de consola realiza las siguientes solicitudes a la API para la funcionalidad básica de NetApp Backup and Recovery :

- Microsoft.Storage/storageAccounts/listkeys/acción
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/cuentasDeAlmacenamiento/escritura
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/acción
- Microsoft.Recursos/suscripciones/ubicaciones/lectura
- Microsoft.Recursos/suscripciones/gruposderecursos/lectura
- Microsoft.Recursos/suscripciones/grupos de recursos/recursos/lectura

- Microsoft.Recursos/suscripciones/gruposderecursos/escritura
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Autorización/bloqueos/escritura
- Microsoft.Authorization/locks/read

La siguiente es una política personalizada para Copia de seguridad y recuperación que utiliza el menor número posible de permisos y el alcance más reducido posible:

```
{
  "id":
"/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDef
initions/{roleDefinitionGuid}",
  "properties": {
    "roleName": "Custom Role",
    "description": "Minimal permissions required for Backup and
Recovery.",
    "assignableScopes": [
      "/subscriptions/{subscriptionId}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}/providers/Microsoft.Storage/storageAccounts/
{storageAccountNameWithObjectLockPreprovisioned}"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/write",
          "Microsoft.Authorization/locks/write",
          "Microsoft.Authorization/locks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

Permisos avanzados de copia de seguridad y recuperación

El agente de consola realiza las siguientes solicitudes de API para operaciones avanzadas de copia de seguridad y recuperación, así como para funciones de búsqueda y restauración. Estos permisos permiten la gestión de redes, almacenes de claves e identidades gestionadas:

- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.KeyVault/vaults/lectura
- Microsoft.ManagedIdentity/userAssignedIdentities/asignar/acción
- Microsoft.Network/networkInterfaces/eliminar
- Microsoft.Network/networkInterfaces/read
- Microsoft.Network/networkSecurityGroups/eliminar
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/virtualNetworks/join/acción
- Microsoft.Recursos/implementaciones/eliminar

Permisos heredados para Copia de seguridad y recuperación

El agente realiza las siguientes solicitudes a la API cuando usted utiliza la funcionalidad de Búsqueda y Restauración. Solo necesita estos permisos si habilitó las funciones de indexación heredadas antes del lanzamiento de la indexación v2 en febrero de 2025:

- Microsoft.Synapse/espacios de trabajo/escritura
- Microsoft.Synapse/espacios de trabajo/lectura
- Microsoft.Synapse/espacios de trabajo/eliminar
- Microsoft.Synapse/registrar/acción
- Microsoft.Synapse/checkNameAvailability/acción
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/acción
- Microsoft.Synapse/espacios de trabajo/resultadosdeoperación/lectura
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/acción

NetApp Data Classification

El agente realiza las siguientes solicitudes de API cuando utiliza la clasificación de datos.

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Compute/ubicaciones/operaciones/lectura	Sí	Sí

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Compute/ubicaciones/vmSizes/lectura	Sí	Sí
Microsoft.Compute/operaciones/lectura	Sí	Sí
Microsoft.Compute/virtualMachines/instanceView/read	Sí	Sí
Microsoft.Compute/virtualMachines/powerOff/acción	Sí	No
Microsoft.Compute/virtualMachines/read	Sí	Sí
Microsoft.Compute/virtualMachines/reiniciar/acción	Sí	No
Microsoft.Compute/virtualMachines/start/action	Sí	No
Microsoft.Compute/virtualMachines/vmSizes/read	No	Sí
Microsoft.Compute/virtualMachines/write	Sí	No
Microsoft.Compute/imágenes/lectura	Sí	Sí
Microsoft.Compute/discos/eliminar	Sí	No
Microsoft.Compute/discos/lectura	Sí	Sí
Microsoft.Compute/discos/escritura	Sí	No
Microsoft.Storage/checknameavailability/read	Sí	Sí
Microsoft.Storage/operaciones/lectura	Sí	Sí
Microsoft.Storage/storageAccounts/listkeys/acción	Sí	No
Microsoft.Storage/storageAccounts/read	Sí	Sí
Microsoft.Storage/cuentasDeAlmacenamiento/escritura	Sí	No
Microsoft.Storage/storageAccounts/blobServices/containers/read	Sí	Sí
Microsoft.Network/networkInterfaces/read	Sí	Sí
Microsoft.Network/interfacesdered/escritura	Sí	No

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Network/networkInterfaces/join/acción	Sí	No
Microsoft.Network/networkSecurityGroups/read	Sí	Sí
Microsoft.Network/networkSecurityGroups/write	Sí	No
Microsoft.Recursos/suscripciones/ubicaciones/lectura	Sí	Sí
Microsoft.Network/ubicaciones/resultadosdeoperación/lectura	Sí	Sí
Microsoft.Network/ubicaciones/operaciones/lectura	Sí	Sí
Microsoft.Network/virtualNetworks/read	Sí	Sí
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Sí	Sí
Microsoft.Network/virtualNetworks/subnets/read	Sí	Sí
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Sí	Sí
Microsoft.Network/virtualNetworks/virtualMachines/read	Sí	Sí
Microsoft.Network/virtualNetworks/subnets/join/action	Sí	No
Microsoft.Network/virtualNetworks/subnets/write	Sí	No
Microsoft.Network/routeTables/join/acción	Sí	No
Microsoft.Recursos/implementaciones/operaciones/lectura	Sí	Sí
Microsoft.Recursos/implementaciones/lectura	Sí	Sí
Microsoft.Recursos/implementaciones/escritura	Sí	No
Microsoft.Recursos/recursos/leer	Sí	Sí
Microsoft.Recursos/suscripciones/resultadosdeoperación/lectura	Sí	Sí
Microsoft.Recursos/suscripciones/gruposderecursos/eliminar	Sí	No

Acción	¿Se utiliza para la configuración?	¿Se utiliza para operaciones diarias?
Microsoft.Recursos/suscripciones/gruposderecursos/lectura	Sí	Sí
Microsoft.Recursos/suscripciones/grupos de recursos/recursos/lectura	Sí	Sí
Microsoft.Recursos/suscripciones/gruposderecursos/escritura	Sí	No

Cloud Volumes ONTAP

El agente realiza las siguientes solicitudes de API para implementar y administrar Cloud Volumes ONTAP en Azure.

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Crear y administrar máquinas virtuales	Microsoft.Compute/ubicaciones/operaciones/lectura	Sí	Sí	No
	Microsoft.Compute/ubicaciones/vmSizes/lectura	Sí	Sí	No
	Microsoft.Recursos/suscripciones/ubicaciones/lectura	Sí	No	No
	Microsoft.Compute/operaciones/lectura	Sí	Sí	No
	Microsoft.Compute/virtualMachines/instanceView/read	Sí	Sí	No
	Microsoft.Compute/virtualMachines/powerOff/acción	Sí	Sí	No
	Microsoft.Compute/virtualMachines/read	Sí	Sí	No
	Microsoft.Compute/virtualMachines/reiniciar/acción	Sí	Sí	No
	Microsoft.Compute/virtualMachines/start/action	Sí	Sí	No
	Microsoft.Compute/virtualMachines/desasignar/acción	No	Sí	Sí
	Microsoft.Compute/virtualMachines/vmSizes/read	No	Sí	No
	Microsoft.Compute/virtualMachines/write	Sí	Sí	No
	Microsoft.Compute/virtualMachines/eliminar	Sí	Sí	Sí
	Microsoft.Recursos/implementaciones/eliminar	Sí	No	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Habilitar la implementación desde un VHD	Microsoft.Compute/imágenes/lectura	Sí	No	No
	Microsoft.Compute/imágenes/escritura	Sí	No	No
Crear y administrar interfaces de red en la subred de destino	Microsoft.Network/networkInterfaces/read	Sí	Sí	No
	Microsoft.Network/interfacesdered/escritura	Sí	Sí	No
	Microsoft.Network/networkInterfaces/join/acción	Sí	Sí	No
	Microsoft.Network/networkInterfaces/eliminar	Sí	Sí	No
Crear y administrar grupos de seguridad de red	Microsoft.Network/networkSecurityGroups/read	Sí	Sí	No
	Microsoft.Network/networkSecurityGroups/write	Sí	Sí	No
	Microsoft.Network/networkSecurityGroups/join/acción	Sí	No	No
	Microsoft.Network/networkSecurityGroups/eliminar	No	Sí	Sí

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Obtenga información de red sobre las regiones, la red virtual y la subred de destino, y agregue las máquinas virtuales a las redes virtuales	Microsoft.Network/ubicaciones/resultadosdeoperación/lectura	Sí	Sí	No
	Microsoft.Network/ubicaciones/operaciones/lectura	Sí	Sí	No
	Microsoft.Network/virtualNetworks/read	Sí	No	No
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Sí	No	No
	Microsoft.Network/virtualNetworks/subnets/read	Sí	Sí	No
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Sí	Sí	No
	Microsoft.Network/virtualNetworks/virtualMachines/read	Sí	Sí	No
	Microsoft.Network/virtualNetworks/subnets/join/action	Sí	Sí	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Crear y administrar grupos de recursos	Microsoft.Recursos/implementaciones/operaciones/lectura	Sí	Sí	No
	Microsoft.Recursos/implementaciones/lectura	Sí	Sí	No
	Microsoft.Recursos/implementaciones/escritura	Sí	Sí	No
	Microsoft.Recursos/recursos/leer	Sí	Sí	No
	Microsoft.Recursos/suscripciones/resultadosdeoperación/lectura	Sí	Sí	No
	Microsoft.Recursos/suscripciones/gruposderecursos/eliminar	Sí	Sí	Sí
	Microsoft.Recursos/suscripciones/gruposderecursos/lectura	No	Sí	No
	Microsoft.Recursos/suscripciones/gruposde recursos/recursos/lectura	Sí	Sí	No
	Microsoft.Recursos/suscripciones/gruposderecursos/escritura	Sí	Sí	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Administrar cuentas y discos de almacenamiento de Azure	Microsoft.Compute/discos/lectura	Sí	Sí	Sí
	Microsoft.Compute/discos/escritura	Sí	Sí	No
	Microsoft.Compute/discos/eliminar	Sí	Sí	Sí
	Microsoft.Storage/checknameavailability/read	Sí	Sí	No
	Microsoft.Storage/operaciones/lectura	Sí	Sí	No
	Microsoft.Storage/storageAccounts/listkeys/acción	Sí	Sí	No
	Microsoft.Storage/storageAccounts/read	Sí	Sí	No
	Microsoft.Storage/cuentasDeAlmacenamiento/eliminar	No	Sí	Sí
	Microsoft.Storage/cuentasDeAlmacenamiento/escritura	Sí	Sí	No
	Microsoft.Storage/usos/lectura	No	Sí	No
Habilitar copias de seguridad en el almacenamiento de blobs y el cifrado de cuentas de almacenamiento	Microsoft.Storage/storageAccounts/blobServices/containers/read	Sí	Sí	No
	Microsoft.KeyVault/vaults/lectura	Sí	Sí	No
	Microsoft.KeyVault/vaults/accessPolicies/write	Sí	Sí	No
Habilitar puntos finales de servicio de VNet para la organización en niveles de datos	Microsoft.Network/virtualNetworks/subnets/write	Sí	Sí	No
	Microsoft.Network/routeTables/join/acción	Sí	Sí	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Crear y administrar instantáneas administradas de Azure	Microsoft.Compute/instantáneas/escritura	Sí	Sí	No
	Microsoft.Compute/instantáneas/lectura	Sí	Sí	No
	Microsoft.Compute/instantáneas/eliminar	No	Sí	Sí
	Microsoft.Compute/disks/beginGetAccess/acción	No	Sí	No
Crear y administrar conjuntos de disponibilidad	Microsoft.Compute/conjuntosdedisponibilidad/escritura	Sí	No	No
	Microsoft.Compute/conjuntosdedisponibilidad/lectura	Sí	No	No
Habilitar implementaciones programáticas desde el mercado	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/planes/agreements/read	Sí	No	No
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/planes/agreements/write	Sí	Sí	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Administrar un balanceador de carga para pares de alta disponibilidad	Microsoft.Network/balanceadoresdecarga/lectura	Sí	Sí	No
	Microsoft.Network/balanceadoresdecarga/escritura	Sí	No	No
	Microsoft.Network/balanceadoresdecarga/eliminar	No	Sí	Sí
	Microsoft.Network/loadBalancers/backendAddressPools/read	Sí	No	No
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Sí	No	No
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	Sí	Sí	No
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Sí	No	No
	Microsoft.Network/loadBalancers/probes/read	Sí	No	No
	Microsoft.Network/loadBalancers/probes/join/action	Sí	No	No
Habilitar la administración de bloqueos en discos de Azure	Microsoft.Autorización/bloqueos/*	Sí	Sí	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Habilite puntos finales privados para pares de alta disponibilidad cuando no haya conectividad fuera de la subred	Microsoft.Network/privateEndpoints/write	Sí	Sí	No
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acción	Sí	No	No
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	Sí	Sí	Sí
	Microsoft.Network/privateEndpoints/read	Sí	Sí	Sí
	Microsoft.Network/privateDnsZones/write	Sí	Sí	No
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Sí	Sí	No
	Microsoft.Network/virtualNetworks/join/acción	Sí	Sí	No
	Microsoft.Network/privateDnsZones/A/write	Sí	Sí	No
	Microsoft.Network/privateDnsZones/read	Sí	Sí	No
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Sí	Sí	No
Necesario para algunas implementaciones de máquinas virtuales, según el hardware físico subyacente	Microsoft.Recursos/implementaciones/estadosdeoperación/lectura	Sí	Sí	No
Eliminar recursos de un grupo de recursos en caso de falla o eliminación de la implementación	Microsoft.Network/privateEndpoints/eliminar	Sí	Sí	No
	Microsoft.Compute/disponibilidadConjuntos/eliminar	Sí	Sí	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Habilitar el uso de claves de cifrado administradas por el cliente al utilizar la API	Microsoft.Compute/diskEncryptionSets/lectura	Sí	Sí	Sí
	Microsoft.Compute/diskEncryptionSets/write	Sí	Sí	No
	Microsoft.KeyVault/vaults/deploy/action	Sí	No	No
	Microsoft.Compute/diskEncryptionSets/eliminar	Sí	Sí	Sí
Configurar un grupo de seguridad de aplicaciones para un par de alta disponibilidad (HA) para aislar la interconexión de HA y las NIC de red del clúster	Microsoft.Network/applicationSecurityGroups/write	No	Sí	No
	Microsoft.Network/applicationSecurityGroups/read	No	Sí	No
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/acción	No	Sí	No
	Microsoft.Network/networkSecurityGroups/securityRules/write	Sí	Sí	No
	Microsoft.Network/applicationSecurityGroups/eliminar	No	Sí	Sí
	Microsoft.Network/networkSecurityGroups/securityRules/eliminar	No	Sí	Sí
Leer, escribir y eliminar etiquetas asociadas con los recursos de Cloud Volumes ONTAP	Microsoft.Recursos/etiquetas/leer	No	Sí	No
	Microsoft.Recursos/etiquetas/escritura	Sí	Sí	No
	Microsoft.Resources/etiquetas/eliminar	Sí	No	No
Cifrar cuentas de almacenamiento durante la creación	Microsoft.ManagedIdentity/userAssignedIdentities/asignar/acción	Sí	Sí	No

Objetivo	Acción	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
Utilice conjuntos de escala de máquinas virtuales en el modo de orquestación flexible para especificar zonas específicas para Cloud Volumes ONTAP	Microsoft.Compute/virtualMachineScaleSets/write	Sí	No	No
	Microsoft.Compute/virtualMachineScaleSets/lectura	Sí	No	No
	Microsoft.Compute/virtualMachineScaleSets/eliminar	No	No	Sí

Nivelación

El agente realiza las siguientes solicitudes de API cuando configura NetApp Cloud Tiering.

- Microsoft.Storage/storageAccounts/listkeys/acción
- Microsoft.Recursos/suscripciones/gruposderecursos/lectura
- Microsoft.Recursos/suscripciones/ubicaciones/lectura

El agente de consola realiza las siguientes solicitudes de API para las operaciones diarias.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/read

Registro de cambios

A medida que se agreguen y eliminen permisos, los indicaremos en las secciones siguientes.

11 de noviembre de 2025

Se agregó una política JSON personalizada que refleja la menor cantidad de permisos posibles y el alcance más estrecho posible.

Se agregaron los siguientes permisos a la lista mínima de permisos de copia de seguridad y recuperación:

- Microsoft.Autorización/bloqueos/escritura
- Microsoft.Authorization/locks/read

Los siguientes permisos ya no son necesarios para Copia de seguridad y recuperación a menos que utilice la indexación heredada:

- Microsoft.Synapse/espacios de trabajo/escritura
- Microsoft.Synapse/espacios de trabajo/lectura
- Microsoft.Synapse/espacios de trabajo/eliminar

- Microsoft.Synapse/registrar/acción
- Microsoft.Synapse/checkNameAvailability/acción
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/acción
- Microsoft.Synapse/espacios de trabajo/resultadosdeoperación/lectura
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/acción

Los siguientes permisos se han movido a la sección "Permisos adicionales de copia de seguridad y recuperación" porque no son necesarios para una configuración mínima:

- Microsoft.Storage/storageAccounts/listkeys/acción
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/cuentasDeAlmacenamiento/escritura
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/acción
- Microsoft.Recursos/suscripciones/ubicaciones/lectura
- Microsoft.Recursos/suscripciones/gruposderecursos/lectura
- Microsoft.Recursos/suscripciones/grupos de recursos/recursos/lectura
- Microsoft.Recursos/suscripciones/gruposderecursos/escritura
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write

9 de septiembre de 2024

Los siguientes permisos se eliminaron de la política JSON porque la consola ya no admite el descubrimiento y la administración de clústeres de Kubernetes:

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/acción
- Microsoft.ContainerService/managedClusters/lectura

22 de agosto de 2024

Se agregaron los siguientes permisos a la política JSON porque son necesarios para la compatibilidad de Cloud Volumes ONTAP con conjuntos de escalado de máquinas virtuales:

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/lectura
- Microsoft.Compute/virtualMachineScaleSets/eliminar

5 de diciembre de 2023

Los siguientes permisos ya no son necesarios para NetApp Backup and Recovery al realizar copias de seguridad de datos de volumen en Azure Blob Storage:

- Microsoft.Compute/virtualMachines/read

- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/desasignar/acción
- Microsoft.Compute/virtualMachines/extensiones/eliminar
- Microsoft.Compute/virtualMachines/eliminar

Estos permisos son necesarios para otros servicios de almacenamiento de la consola, por lo que permanecerán en la función personalizada para el agente si está utilizando esos otros servicios de almacenamiento.

12 de mayo de 2023

Se agregaron los siguientes permisos a la política JSON porque son necesarios para la administración de Cloud Volumes ONTAP :

- Microsoft.Compute/imágenes/escritura
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

Los siguientes permisos se eliminaron de la política JSON porque ya no son necesarios:

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/eliminar

23 de marzo de 2023

El permiso "Microsoft.Storage/storageAccounts/delete" ya no es necesario para la clasificación de datos.

Este permiso aún es necesario para Cloud Volumes ONTAP.

5 de enero de 2023

Se agregaron los siguientes permisos a la política JSON:

- Microsoft.Storage/storageAccounts/listAccountSas/acción
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/acción

  Estos permisos son necesarios para NetApp Backup and Recovery.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  Este permiso es necesario para la implementación de Cloud Volumes ONTAP .

Reglas del grupo de seguridad del agente de consola en Azure

El grupo de seguridad de Azure para el agente requiere reglas de entrada y de salida. La NetApp Console crea automáticamente este grupo de seguridad cuando crea un agente de consola desde la consola. Para otras opciones de instalación, debe configurar este grupo de seguridad manualmente.

Reglas de entrada

Protocolo	Puerto	Objetivo
SSH	22	Proporciona acceso SSH al host del agente
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 y conexiones desde la instancia de NetApp Data Classification
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet para enviar mensajes de AutoSupport al soporte de NetApp . Debe abrir este puerto manualmente después de la implementación. "Descubra cómo se utiliza el agente como proxy para los mensajes de AutoSupport"

Reglas de salida

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

Reglas básicas de salida

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

Protocolo	Puerto	Objetivo
Todo TCP	Todo	Todo el tráfico saliente
Todos los UDP	Todo	Todo el tráfico saliente

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

Servicio	Protocolo	Puerto	Destino	Objetivo
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres ONTAP e Internet saliente	Llamadas API a Azure, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp
Llamadas API	TCP	8080	Clasificación de datos	Sonda a la instancia de clasificación de datos durante la implementación
DNS	UDP	53	DNS	Utilizado para la resolución de DNS por la consola

Permisos de Google Cloud y reglas de firewall requeridas

Permisos de Google Cloud para el agente de la consola

El agente de la consola requiere permisos para realizar acciones en Google Cloud. Estos permisos están incluidos en una función personalizada proporcionada por NetApp. Debes comprender qué hace el agente con estos permisos.

Permisos de la cuenta de usuario de Google Cloud

La siguiente función personalizada otorga a un usuario de Google Cloud los permisos necesarios para implementar un agente. Aplique este rol personalizado al usuario que implementará el agente.

Ver los permisos de la cuenta de usuario de Google Cloud

```
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
```

Permisos de la cuenta de servicio

La función personalizada a continuación le otorga a la cuenta de servicio de Google Cloud asociada al agente de la consola los permisos necesarios para administrar recursos y procesos en su red de Google Cloud.

Aplique esta función personalizada a una cuenta de servicio asociada a la máquina virtual del agente de

consola.

- "Configurar los permisos de Google Cloud para el modo estándar"
- "Configurar permisos para el modo restringido"

Ver los permisos de la cuenta de servicio de Google

Asegúrese de que la función esté actualizada a medida que se agreguen o eliminen nuevos permisos en versiones posteriores. El registro de cambios enumera todos los nuevos permisos necesarios."Revisar el registro de cambios de permisos de Google" "Revisa cómo agregar cuentas de servicio de Google Cloud"

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent.
stage: GA
includedPermissions:
- cloudbuild.builds.get
- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
- config.artifacts.import
- config.deployments.create
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getLock
- config.deployments.getState
- config.deployments.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.deployments.getLock
- config.deployments.list
- config.deployments.lock
- config.operations.get
- config.previews.get
- config.previews.list
- config.resources.list
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionBackendServices.update
- compute.networks.updatePolicy
- compute.addresses.createInternal
```

```
- compute.addresses.deleteInternal
- compute.addresses.list
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.backendServices.create
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- 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.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.forwardingRules.update
- compute.globalOperations.get
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
```

```
- compute.instances.use
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.get
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.instances.setMinCpuPlatform
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.regionBackendServices.delete
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- 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
- logging.logEntries.list
- logging.privateLogEntries.list
- logging.logEntries.create
- logging.logEntries.route
- monitoring.timeSeries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.list
- storage.objects.update
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.get
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.objects.get
- storage.objects.list
- storage.buckets.getIamPolicy
```

Cómo se utilizan los permisos de Google Cloud

El agente de la consola usa los permisos en la función personalizada para administrar los recursos de Cloud Volumes ONTAP y los procesos de servicios de datos de NetApp en su red de Google Cloud. Las siguientes secciones describen cómo el agente utiliza estos permisos.

Permisos utilizados para Cloud Volumes ONTAP

El agente de la consola usa los permisos en la función personalizada para administrar los recursos y procesos de Cloud Volumes ONTAP en su red de Google Cloud. Las siguientes secciones describen cómo el agente utiliza estos permisos.

Permisos para Cloud Volumes ONTAP

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
config.deployments.create	Para implementar la instancia de máquina virtual Cloud Volumes ONTAP mediante Google Cloud Infrastructure Manager.	Sí	No	No
config.deployments.delete		No	No	Sí
config.deployments.deleteState		No	No	Sí
config.deployments.get		No	Sí	No
config.deployments.getLock		No	Sí	No
config.deployments.getState		No	Sí	No
lista de configuraciones de despliegue		No	Sí	No
config.deployments.lock		No	Sí	No
config.deployments.update		No	Sí	No
config.deployments.updateState		No	Sí	No
config.operaciones.get		No	Sí	No
config.previews.get		No	Sí	No
lista de vistas previas de configuración		No	Sí	No
lista de recursos de configuración		No	Sí	No
config.revisions.get		No	Sí	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
crear.discos.computar	Para crear y administrar discos para Cloud Volumes ONTAP.	Sí	Sí	No
compute.disks.createSnapshot		No	Sí	No
eliminar discos de cálculo		No	Sí	Sí
compute.disks.get		No	Sí	No
compute.disks.list		Sí	Sí	No
computar.discos.establecerEtiquetas		Sí	Sí	No
usar discos de cálculo		No	Sí	No
crear.cortafuegos.	Para crear reglas de firewall para Cloud Volumes ONTAP.	Sí	No	No
compute.firewalls.delete		No	Sí	Sí
compute.firewalls.get		Sí	Sí	No
compute.firewalls.list		Sí	Sí	No
calcular.reenvíoReglas.crear	Cree reglas de reenvío para enrutar el tráfico hacia los servicios backend.	No	Sí	No
calcular.reenvíoReglas.eliminar	Eliminar reglas de reenvío existentes.	No	Sí	No
calcular.reenvíoReglas.obtener	Recupere detalles sobre las reglas de reenvío existentes.	No	Sí	No
calcular.reenvíoReglas.establecerEtiquetas	Establecer o actualizar etiquetas en las reglas de reenvío para la organización.	No	Sí	No
compute.forwardingRules.update	Actualiza las reglas de reenvío existentes para la gestión del tráfico.	No	Sí	No
computar.globalOperations.get	Para obtener el estado de las operaciones.	Sí	Sí	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
computar.healthChecks.crear	Cree y administre controles de estado para supervisar el estado del servicio backend.	No	Sí	No
computar.healthChecks.eliminar		No	Sí	No
computar.healthChecks.get		No	Sí	No
computar.healthChecks.useReadOnly		No	Sí	No
compute.images.get	Para obtener imágenes para instancias de VM.	Sí	No	No
compute.images.getFromFamily		Sí	No	No
compute.images.list		Sí	No	No
compute.images.useReadOnly		Sí	No	No
compute.instances.attachDisk	Para conectar y desconectar discos a Cloud Volumes ONTAP.	Sí	Sí	No
compute.instances.detachDisk		No	Sí	Sí
crear instancias de cómputo	Para crear y eliminar instancias de VM de Cloud Volumes ONTAP .	Sí	No	No
compute.instances.delete		No	No	Sí
compute.instances.get	Para enumerar instancias de VM.	Sí	Sí	No
compute.instances.getSerialPortOutput	Para obtener registros de la consola.	Sí	Sí	No
compute.instances.list	Para recuperar la lista de instancias en una zona.	Sí	Sí	No
compute.instances.setDeletionProtection	Para establecer la protección contra eliminación en la instancia.	Sí	No	No
compute.instances.setLabels	Para agregar etiquetas.	Sí	No	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
compute.instances.setMachineType	Para cambiar el tipo de máquina para Cloud Volumes ONTAP.	Sí	Sí	No
compute.instances.setMinCpuPlatform		Sí	Sí	No
compute.instances.setMetadata	Para agregar metadatos.	Sí	Sí	No
compute.instances.setTags	Para agregar etiquetas para las reglas de firewall.	Sí	Sí	No
compute.instances.start	Para iniciar y detener Cloud Volumes ONTAP.	Sí	Sí	No
compute.instances.stop		Sí	Sí	No
compute.instances.updateDisplayDevice		Sí	Sí	No
computar.instancias.uso	Utilice instancias de máquinas virtuales (operaciones de inicio, detención y conexión).	No	Sí	No
compute.machineTypes.get	Para obtener el número de núcleos y comprobar las cuotas.	Sí	No	No
compute.projects.get	Para apoyar multiproyectos.	Sí	No	No
computar.políticasderecursos.crear	Cree y administre políticas de recursos para la gestión automatizada de recursos.	No	Sí	No
computar.políticasderecursos.eliminar		No	Sí	No
computar.políticasderecursos.obtener		No	Sí	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
crear.instantáneas.computar	Para crear y administrar instantáneas de disco persistentes.	Sí	Sí	No
compute.snapshots.delete		No	Sí	Sí
compute.snapshots.get		No	Sí	No
compute.snapshots.list		No	Sí	No
calcular.instantáneas.establecerEtiquetas		Sí	Sí	No
compute.networks.get	Para obtener la información de red necesaria para crear una nueva instancia de máquina virtual Cloud Volumes ONTAP .	Sí	Sí	No
compute.networks.list		Sí	Sí	No
compute.regions.get		Sí	Sí	No
compute.regions.list		Sí	Sí	No
compute.subnetworks.get		Sí	Sí	No
compute.subnetworks.list		Sí	Sí	No
compute.zoneOperations.get		Sí	Sí	No
compute.zones.get		Sí	Sí	No
compute.zones.list		Sí	Sí	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
deploymentmanager.compositeTypes.get	Para implementar la instancia de máquina virtual Cloud Volumes ONTAP mediante Google Cloud Deployment Manager.	Sí	No	No
deploymentmanager.compositeTypes.list		Sí	No	No
gestor de despliegue.despliegues.crear		Sí	No	No
gestor de despliegue.despliegues.eliminar		Sí	No	No
deploymentmanager.deployments.get		Sí	No	No
deploymentmanager.deployments.list		Sí	No	No
deploymentmanager.manifests.get		Sí	No	No
deploymentmanager.manifests.list		Sí	No	No
deploymentmanager.operations.get		Sí	No	No
lista de operaciones del administrador de despliegue		Sí	No	No
deploymentmanager.resources.get		Sí	No	No
deploymentmanager.resources.list		Sí	No	No
deploymentmanager.typeProviders.get		Sí	No	No
deploymentmanager.typeProviders.list		Sí	No	No
deploymentmanager.types.get		Sí	No	No
lista de tipos de gestor de despliegue		Sí	No	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
logging.logEntries.list	Para obtener unidades de registro de pila.	Sí	Sí	No
logging.privateLogEntries.list		Sí	Sí	No
registro.logEntries.create	Cree y enrute archivos de registro para monitoreo, depuración y auditoría.	Sí	Sí	No
registro.logEntries.route		Sí	Sí	No
resourcemanager.projects.get	Para apoyar multiproyectos.	Sí	Sí	No
almacenamiento.cubos.crear	Para crear y administrar un depósito de Google Cloud Storage para la organización en niveles de datos.	Sí	Sí	No
almacenamiento.cubos.eliminar		No	Sí	Sí
almacenamiento.cubos.obtener		No	Sí	No
lista de cubos de almacenamiento		No	Sí	No
almacenamiento.cubos.actualizar		No	Sí	No
cloudkms.cryptoKeyVersions.useToEncrypt	Para utilizar claves de cifrado administradas por el cliente desde el Servicio de administración de claves en la nube con Cloud Volumes ONTAP.	Sí	Sí	No
cloudkms.cryptoKeys.get		Sí	Sí	No
cloudkms.cryptoKeys.lista		Sí	Sí	No
lista de llaveros cloudkms		Sí	Sí	No
cloudbuild.builds.get		Sí	No	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
compute.instances.setServiceAccount	Para configurar una cuenta de servicio en la instancia de Cloud Volumes ONTAP . Esta cuenta de servicio proporciona permisos para la organización de datos en niveles en un depósito de Google Cloud Storage.	Sí	Sí	No
soy.cuentasdeservicio.actuar como		Sí	No	No
iam.serviceAccounts.create		Sí	No	No
iam.serviceAccounts.getIamPolicy		Sí	Sí	No
soy.serviceAccounts.list		Sí	Sí	No
iam.serviceAccountKeys.create		Sí	No	No
almacenamiento.objetos.crear	Cree y administre objetos (archivos) en el depósito de Google Cloud Storage.	Sí	Sí	No
almacenamiento.objetos.eliminar		No	No	Sí
almacenamiento.objetos.obtener		Sí	Sí	No
almacenamiento.objetos.lista		Sí	Sí	No
calcular.direcciones.lista	Para recuperar las direcciones en una región al implementar un par HA.	Sí	No	No
computar.direcciones.crearInterno	Cree direcciones IP internas dentro de la red VPC para la asignación de recursos.	No	Sí	No
computar.direcciones.eliminarInterno	Eliminar direcciones IP internas para limpiar recursos.	No	Sí	No
calcular.direcciones.establecerEtiquetas	Actualizar etiquetas en el recurso Dirección.	No	Sí	No
computar.direcciones.useInternal	Utilice direcciones IP internas para la comunicación de red.	No	Sí	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
compute.backendServices.create	Configurar un servicio de backend para distribuir el tráfico en un par HA.	Sí	No	No
compute.regionBackendServices.create	Crear y administrar servicios backend para enrutamiento de tráfico.	Sí	No	No
computar.regionBackendServices.eliminar		No	Sí	No
compute.regionBackendServices.get		Sí	No	No
computar.regionBackendServices.update		Sí	Sí	No
compute.regionBackendServices.list		Sí	No	No
computar.regiónBackendServices.uso		No	Sí	No
política de actualización de redes de computación	Para aplicar reglas de firewall en las VPC y subredes de un par de alta disponibilidad.	Sí	No	No
compute.instanceGroups.get	Para crear y administrar máquinas virtuales de almacenamiento en pares HA de Cloud Volumes ONTAP .	Sí	Sí	No
calcular.direcciones.obtener		Sí	Sí	No
computar.instancias.actualizarInterfazDeRed		Sí	Sí	No
computar.gruposdeinstancias.crear		No	Sí	No
calcular.gruposdeinstancias.eliminar		No	Sí	No
computar.gruposdeinstancias.actualizar		No	Sí	No
computar.gruposdeinstancias.uso		No	Sí	No

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
monitorización.lista de series temporales	Para descubrir información sobre los depósitos de Google Cloud Storage.	Sí	Sí	No
almacenamiento.cubos.obtenerPolíticaIam		Sí	Sí	No

Permisos utilizados para NetApp Backup and Recovery

El agente de consola usa los permisos en el rol personalizado para administrar los recursos y procesos de NetApp Backup and Recovery en su red de Google Cloud. Las siguientes secciones describen cómo el agente utiliza estos permisos.

Ver permisos para NetApp Backup and Recovery

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.lista • cloudkms.cryptoKeys.setIamPolicy • cloudkms.keyRings.get • cloudkms.keyRings.getIamPolicy • lista de llaveros cloudkms • cloudkms.keyRings.setIamPolicy	Para seleccionar sus propias claves administradas por el cliente en el asistente de activación de NetApp Backup and Recovery en lugar de utilizar las claves de cifrado administradas por Google predeterminadas.	Sí	Sí	No

Permisos utilizados para la NetApp Data Classification

El agente de consola usa los permisos en la función personalizada para administrar los recursos y procesos de NetApp Data Classification en su red de Google Cloud. Las siguientes secciones describen cómo el agente utiliza estos permisos.

Ver permisos para la NetApp Data Classification

Comportamiento	Objetivo	¿Se utiliza para implementación?	¿Se utiliza para operaciones diarias?	¿Se utiliza para eliminar?
• usar subredes de computación • compute.subnetworks.useExternalIp • compute.instances.addAccessConfig	Para habilitar la NetApp Data Classification.	Sí	No	No

Registro de cambios

Los permisos agregados y eliminados se detallan a continuación.

09 de febrero de 2026

El permiso `compute.forwardingRules.update` se añade para dar soporte a Infrastructure Manager en implementaciones de Cloud Volumes ONTAP en Google Cloud.

08 de diciembre de 2025

NetApp está migrando de Google Cloud Deployment Manager a Google Cloud Infrastructure Manager (IM) para implementar y ejecutar el agente de consola en Google Cloud. Se agregaron los siguientes permisos para respaldar este cambio.

Los siguientes permisos agregados son necesarios para el usuario de Google Cloud que implementa el agente:

- almacenamiento.cubos.crear
- almacenamiento.cubos.obtener
- almacenamiento.objetos.crear
- almacenamiento.carpetas.crear
- almacenamiento.objetos.lista
- iam.serviceAccount.actAs
- config.deployments.create
- config.operaciones.get

Se requieren los siguientes permisos adicionales para la cuenta de servicio en Google Cloud utilizada para las operaciones diarias:

- lista de conexiones de cloudbuild

- cloudbuild.repositories.accessReadToken
- lista de repositorios de cloudbuild
- cloudquotas.quotas.get
- config.artefactos.importar
- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.previews.upload
- config.revisions.getState
- registro.logEntries.create
- almacenamiento.objetos.crear
- almacenamiento.objetos.eliminar
- almacenamiento.objetos.actualizar
- iam.serviceAccounts.get

Se requieren los siguientes permisos agregados para implementar Cloud Volumes ONTAP:

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- lista de configuraciones de despliegue
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- lista de vistas previas de configuración
- config.revisions.get
- lista de recursos de configuración
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

Los siguientes permisos agregados son necesarios para la cuenta de servicio utilizada para las operaciones diarias de Cloud Volumes ONTAP.

- computar.direcciones.crearInterno
- computar.direcciones.eliminarInterno
- calcular.direcciones.establecerEtiquetas
- computar.direcciones.useInternal

- calcular.reenvíoReglas.crear
- calcular.reenvíoReglas.eliminar
- calcular.reenvíoReglas.obtener
- calcular.reenvíoReglas.establecerEtiquetas
- computar.healthChecks.crear
- computar.healthChecks.eliminar
- computar.healthChecks.get
- computar.healthChecks.useReadOnly
- computar.gruposdeinstancias.crear
- calcular.gruposdeinstancias.eliminar
- computar.gruposdeinstancias.actualizar
- computar.gruposdeinstancias.uso
- computar.instancias.uso
- computar.regionBackendServices.eliminar
- computar.regionBackendServices.update
- computar.regiónBackendServices.uso
- computar.políticasderecursos.crear
- computar.políticasderecursos.eliminar
- computar.políticasderecursos.obtener
- registro.logEntries.route
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- config.operaciones.get

26 de noviembre de 2025

Los permisos se han actualizado para aclarar su uso, pero no se han añadido ni eliminado permisos. Se añaden tres columnas para indicar si cada permiso se utiliza para la implementación, las operaciones diarias o la eliminación. Aparte de esto, algunos permisos están segregados en función de su uso para NetApp Data Classification y NetApp Backup and Recovery.

6 de febrero de 2023

Se agregó el siguiente permiso a esta política:

- computar.instancias.actualizarInterfazDeRed

Este permiso es necesario para Cloud Volumes ONTAP.

27 de enero de 2023

Se agregaron los siguientes permisos a esta política:

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Estos permisos son necesarios para NetApp Backup and Recovery.

Reglas de firewall del agente en Google Cloud

Las reglas de firewall de Google Cloud para el agente requieren reglas tanto entrantes como salientes. La NetApp Console crea automáticamente este grupo de seguridad cuando crea un agente de consola desde la consola. Para otras opciones de instalación, debe configurar este grupo de seguridad manualmente.

Reglas de entrada

Protocolo	Puerto	Objetivo
SSH	22	Proporciona acceso SSH al host del agente
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
TCP	3128	Proporciona a Cloud Volumes ONTAP acceso a Internet. Debe abrir este puerto manualmente después de la implementación.

Reglas de salida

Las reglas de firewall predefinidas del agente abren todo el tráfico saliente. Siga las reglas básicas de salida si es aceptable o utilice reglas avanzadas de salida para requisitos más estrictos.

Reglas básicas de salida

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

Protocolo	Puerto	Objetivo
Todo TCP	Todo	Todo el tráfico saliente
Todos los UDP	Todo	Todo el tráfico saliente

Reglas de salida avanzadas

Si necesita reglas rígidas para el tráfico saliente, puede utilizar la siguiente información para abrir solo aquellos puertos que el agente requiere para la comunicación saliente.

La dirección IP de origen es el host del agente.

Servicio	Protocolo	Puerto	Destino	Objetivo
Llamadas API y AutoSupport	HTTPS	443	LIF de gestión de clústeres ONTAP e Internet saliente	Llamadas API a Google Cloud, a ONTAP, a NetApp Data Classification y envío de mensajes de AutoSupport a NetApp
Llamadas API	TCP	8080	Clasificación de datos	Sonda a la instancia de clasificación de datos durante la implementación
DNS	UDP	53	DNS	Se utiliza para la resolución de DNS mediante clasificación de datos

Acceso a la red requerido para 3.9.55 y anteriores

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

Este tema documenta el acceso a la red necesario para las versiones del modo estándar de la NetApp Console 3.9.55 y anteriores. Para conocer los puntos finales necesarios para 4.0.0 y superiores, revise"los puntos finales necesarios para 4.0.0 y superiores" .

Debe configurar el acceso a la red para lo siguiente:

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

Actualice su lista de puntos finales a la lista revisada para 4.0.0 y versiones superiores

A partir de la versión 4.0.0, los agentes de consola requieren menos puntos finales. Las implementaciones existentes anteriores a la versión 4.0.0 siguen siendo compatibles. Después de actualizar a 4.0.0 o posterior, puede eliminar los puntos finales antiguos de su lista de permitidos cuando sea conveniente.

NetApp recomienda actualizar las reglas de firewall para utilizar la lista de puntos finales revisada, que es más pequeña, más segura y más fácil de administrar. NetApp elimina la necesidad de entradas comodín y los puntos finales para actualizaciones de agentes admiten todos los servicios de datos.

Puntos finales para la versión 3.9.55 y anteriores	Puntos finales para 4.0.0 y superiores	Objetivo
• \ https://support.netapp.com • \ https://mysupport.netapp.com	• \ https://mysupport.netapp.com • \ https://signin.b2c.netapp.com • \ https://support.netapp.com	Para obtener licencias y comunicarse con el soporte técnico de NetApp .
• https://*.api.bluexp.netapp.com • \ https://api.bluexp.netapp.com • https://*.cloudmanager.cloud.netapp.com • \ https://cloudmanager.cloud.netapp.com • \ https://netapp-cloud-account.auth0.com • \ https://netapp-cloud-account.us.auth0.com • \ https://console.bluexp.netapp.com • https://*.console.bluexp.netapp.com	• \ 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	Para operaciones diarias.
• https://*.blob.core.windows.net • \ https://cloudmanagerinfraprod.azurecr.io	• \ https://bluexpinfraprod.eastus2.data.azurecr.io • \ https://bluexpinfraprod.azurecr.io	Para obtener imágenes para las actualizaciones del agente de consola.

Pasos

1. Verifique que su agente sea la versión 4.0.0 o superior."Ver la versión del agente."
2. Incluir en la lista blanca los puntos finales en"Puntos finales compatibles con 4.0.0 y superiores" .
3. Reinicie el servicio del administrador de servicios 2 en cada agente ejecutando el siguiente comando:

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

4. Ejecute el siguiente comando y verifique que el estado del agente se muestre como *activo(en ejecución)*: _

```
systemctl status netapp-service-manager.service
```

5. Elimina los puntos finales antiguos de la lista de permitidos de tu firewall.

Puntos finales para la NetApp Console y los agentes de consola para la versión 3.9.55 y anteriores

Estos puntos finales se utilizan para agentes de consola 3.9.55 y anteriores.

Puntos finales	Objetivo
\ https://support.netapp.com \ https://mysupport.netapp.com	Para obtener información de licencias y enviar mensajes de AutoSupport al soporte de NetApp .
https://*.api.bluexp.netapp.com \ https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com \ https://cloudmanager.cloud.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com	Proporcionar funciones y servicios dentro de la NetApp Console.
Elija entre dos conjuntos de puntos finales: • Opción 1 (recomendada) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Opción 2 https://*.blob.core.windows.net\ https://cloudmanagerinfraprod.azurecr.io	Para obtener imágenes para las actualizaciones del agente de consola. NetApp recomienda permitir los puntos finales de la Opción 1 en su firewall, ya que son más seguros, y no permitir los puntos finales de la Opción 2, a menos que esté usando Ransomware Resilience o Backup and Recovery. Tenga en cuenta lo siguiente acerca de estos puntos finales: • Los puntos finales de la opción 1 son compatibles con 3.9.47 y versiones posteriores. Las versiones anteriores a 3.9.47 no admiten compatibilidad con versiones anteriores. • El agente de consola inicia primero el contacto con los puntos finales en la opción 2. Si esos puntos finales no son accesibles, se contacta automáticamente con los puntos finales de la opción 1. • Si utiliza el agente de consola con NetApp Backup and Recovery o Ransomware Resilience, el sistema no admite puntos finales de la Opción 1. Permitir puntos finales de la Opción 2 y no permitir la Opción 1.

Puntos finales del proveedor de la nube contactados por el agente de la consola

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

Habilite el acceso a los puntos finales del proveedor de nube antes de instalar el agente de consola.

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

Los puntos finales del proveedor de nube son los mismos para todas las versiones.

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

El agente de consola requiere acceso a Internet saliente adicional para admitir algunos servicios de datos de NetApp y Cloud Volumes ONTAP.

Puntos finales para Cloud Volumes ONTAP

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

Requerir el uso de IMDSv2 en instancias de Amazon EC2

La NetApp Console admite el servicio de metadatos de instancia de Amazon EC2 versión 2 (IMDSv2) con el agente de consola y con Cloud Volumes ONTAP (incluido el mediador para implementaciones de alta disponibilidad). En la mayoría de los casos, IMDSv2 se configura automáticamente en las nuevas instancias EC2. IMDSv1 se habilitó antes de marzo de 2024. Si sus políticas de seguridad lo requieren, es posible que deba configurar manualmente IMDSv2 en sus instancias EC2.

Antes de empezar

- La versión del agente de consola debe ser 3.9.38 o posterior.
- Cloud Volumes ONTAP debe ejecutar una de las siguientes versiones:
  - 9.12.1 P2 (o cualquier parche posterior)
  - 9.13.0 P4 (o cualquier parche posterior)
  - 9.13.1 o cualquier versión posterior a esta
- Este cambio requiere que reinicie las instancias de Cloud Volumes ONTAP .
- Estos pasos requieren el uso de AWS CLI porque debe cambiar el límite de saltos de respuesta a 3.

Acerca de esta tarea

IMDSv2 proporciona protección mejorada contra vulnerabilidades. "Obtenga más información sobre IMDSv2 en el blog de seguridad de AWS."

El Servicio de metadatos de instancia (IMDS) se habilita de la siguiente manera en las instancias EC2:

- Para nuevas implementaciones de agentes de consola desde la consola o mediante "Scripts de Terraform" IMDSv2 está habilitado de forma predeterminada en la instancia EC2.
- Si lanza una nueva instancia EC2 en AWS y luego instala manualmente el software del agente de consola, IMDSv2 también estará habilitado de forma predeterminada.
- Si inicia el agente de consola desde AWS Marketplace, IMDSv1 estará habilitado de forma

predeterminada. Puede configurar manualmente IMDSv2 en la instancia EC2.

- Para los agentes de consola existentes, IMDSv1 aún es compatible, pero puede configurar manualmente IMDSv2 en la instancia EC2 si lo prefiere.
- Para Cloud Volumes ONTAP, IMDSv1 está habilitado de forma predeterminada en instancias nuevas y existentes. Puede configurar manualmente IMDSv2 en las instancias EC2 si lo prefiere.

Pasos

1. Requerir el uso de IMDSv2 en la instancia del agente de consola:

   a. Conéctese a la máquina virtual Linux para el agente de consola.

      Cuando creó la instancia del agente de consola en AWS, proporcionó una clave de acceso y una clave secreta de AWS. Puede utilizar este par de claves para conectarse mediante SSH a la instancia. El nombre de usuario para la instancia EC2 Linux es ubuntu (para los agentes de consola creados antes de mayo de 2023, el nombre de usuario era ec2-user).

      "Documentación de AWS: Conéctese a su instancia de Linux"

   b. Instalar la AWS CLI.

      "Documentación de AWS: Instalar o actualizar a la última versión de la AWS CLI"

   c. Utilice el `aws ec2 modify-instance-metadata-options` comando para requerir el uso de IMDSv2 y cambiar el límite de saltos de respuesta PUT a 3.

      Ejemplo

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

   +

   El `http-tokens` conjuntos de parámetros IMDSv2 como obligatorios. Cuando `http-tokens` es obligatorio, también debes configurar `http-endpoint` para habilitar.

2. Requerir el uso de IMDSv2 en instancias de Cloud Volumes ONTAP :

   a. Ir a la "Consola de Amazon EC2"

   b. Desde el panel de navegación, seleccione **Instancias**.

   c. Seleccione una instancia de Cloud Volumes ONTAP .

   d. Seleccione **Acciones > Configuración de instancia > Modificar opciones de metadatos de instancia**.

   e. En el cuadro de diálogo **Modificar opciones de metadatos de instancia**, seleccione lo siguiente:

      - Para **Servicio de metadatos de instancia**, seleccione **Habilitar**.
      - Para **IMDSv2**, seleccione **Obligatorio**.

- Seleccione **Guardar**.

f. Repita estos pasos para otras instancias de Cloud Volumes ONTAP , incluido el mediador de HA.

g. "Detener e iniciar las instancias de Cloud Volumes ONTAP"

Resultado

La instancia del agente de consola y las instancias de Cloud Volumes ONTAP ahora están configuradas para usar IMDSv2.

Configuración predeterminada para el agente de consola

Obtenga información sobre las configuraciones predeterminadas del agente de consola para implementaciones estándar (con acceso a Internet) en AWS, Azure y Google Cloud, así como para implementaciones restringidas (sin acceso a Internet) en entornos locales.

Configuración predeterminada con acceso a Internet

Los siguientes detalles de configuración se aplican si implementó un agente de consola desde la NetApp Console, desde el mercado de su proveedor de nube o si instaló manualmente un agente de consola en un host Linux local que tiene acceso a Internet.

Detalles de la máquina virtual del agente de consola para AWS

Si implementó un agente de consola desde la consola o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de instancia EC2 es t3.2xlarge.
- El sistema operativo de la imagen es Ubuntu 22.04 LTS.

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

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El nombre de usuario para la instancia EC2 Linux es ubuntu (para los agentes creados antes de mayo de 2023, el nombre de usuario es ec2-user).
- El disco del sistema predeterminado es un disco gp2 de 100 GiB.

Detalles de la máquina virtual del agente de consola para Azure

Si implementó un agente de consola desde la consola o desde el mercado del proveedor de la nube, tenga en cuenta lo siguiente:

- El tipo de VM es Standard_D8s_v3.
- El sistema operativo de la imagen es Ubuntu 22.04 LTS.

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

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El disco del sistema predeterminado es un disco SSD premium de 100 GiB.

Detalles de la máquina virtual del agente de consola para Google Cloud

Si implementó un agente de consola desde la consola, tenga en cuenta lo siguiente:

- La instancia de VM es n2-standard-8.
- El sistema operativo de la imagen es Ubuntu 22.04 LTS.

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

- La instalación incluye Docker Engine, que es la herramienta de orquestación de contenedores necesaria.
- El disco del sistema predeterminado es un disco persistente SSD de 100 GiB.

Carpeta de instalación

La carpeta de instalación del agente se encuentra en la siguiente ubicación:

`/opt/application/netapp/cloudmanager`

Archivos de registro

Los archivos de registro se encuentran en las siguientes carpetas:

- `/opt/application/netapp/cloudmanager/log` o
- `/opt/application/netapp/service-manager-2/logs` (a partir de las nuevas instalaciones 3.9.23)

  Los registros de estas carpetas proporcionan detalles sobre el agente de la consola.

- `/opt/application/netapp/cloudmanager/docker_occm/data/log`

  Los registros de esta carpeta proporcionan detalles sobre los servicios en la nube y el servicio de consola que se ejecuta en el agente de consola.

Servicio de agente de consola

- El servicio del agente de consola se llama occm.
- El servicio occm depende del servicio MySQL.

  Si el servicio MySQL está inactivo, entonces el servicio occm también estará inactivo.

Puertos

El agente utiliza los siguientes puertos en el host Linux:

- 80 para acceso HTTP
- 443 para acceso HTTPS

Configuración predeterminada sin acceso a Internet

La siguiente configuración se aplica si instaló manualmente el agente de consola en un host Linux local que no tiene acceso a Internet. "Obtenga más información sobre esta opción de instalación" .

- La carpeta de instalación del agente se encuentra en la siguiente ubicación:

  `/opt/application/netapp/ds`

- Los archivos de registro se encuentran en las siguientes carpetas:

  `/var/lib/docker/volumes/ds_occmdata/_data/log`

  Los registros de esta carpeta proporcionan detalles sobre el agente de la consola y las imágenes de Docker.

- Todos los servicios se ejecutan dentro de contenedores Docker

  Los servicios dependen del servicio de tiempo de ejecución de Docker que se esté ejecutando

- El agente utiliza los siguientes puertos en el host Linux:
  - 80 para acceso HTTP
  - 443 para acceso HTTPS

Conocimiento y apoyo

Regístrese para recibir asistencia

Es necesario registrarse para recibir soporte técnico específico para la NetApp Console y sus soluciones de almacenamiento y servicios de datos. También es necesario registrarse para obtener soporte técnico para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP .

Registrarse para recibir soporte no habilita el soporte de NetApp para un servicio de archivos de un proveedor de nube. Para obtener asistencia técnica relacionada con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte "Obtener ayuda" en la documentación de ese producto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Descripción general del registro de soporte

Existen dos formas de registro para activar el derecho a recibir ayuda:

- Registrar el número de serie de su cuenta de la NetApp Console (su número de serie 960xxxxxxxxx de 20 dígitos ubicado en la página Recursos de soporte en la consola).

  Esto sirve como su ID de suscripción de soporte único para cualquier servicio dentro de la Consola. Cada cuenta de consola debe estar registrada.

- Registrar los números de serie de Cloud Volumes ONTAP asociados con una suscripción en el mercado de su proveedor de nube (son números de serie 909201xxxxxxxx de 20 dígitos).

  Estos números de serie se conocen comúnmente como *números de serie PAYGO* y son generados por la NetApp Console en el momento de la implementación de Cloud Volumes ONTAP .

El registro de ambos tipos de números de serie permite funciones como la apertura de tickets de soporte y la generación automática de casos. El registro se completa agregando cuentas del sitio de soporte de NetApp (NSS) a la consola como se describe a continuación.

Registrar la NetApp Console para obtener soporte de NetApp

Para registrarse para recibir soporte y activar el derecho a soporte, un usuario de su cuenta de NetApp Console debe asociar una cuenta del sitio de soporte de NetApp con su inicio de sesión de consola. La forma de registrarse para el soporte de NetApp depende de si ya tiene una cuenta del sitio de soporte de NetApp (NSS).

Cliente existente con una cuenta NSS

Si es cliente de NetApp con una cuenta NSS, simplemente necesita registrarse para recibir soporte a través de la consola.

Pasos

1. Seleccione **Administración** > **Credenciales**.
2. Seleccione **Credenciales de usuario**.
3. Seleccione **Agregar credenciales NSS** y siga las instrucciones de autenticación del Sitio de soporte de NetApp (NSS).
4. Para confirmar que el proceso de registro fue exitoso, seleccione el ícono de Ayuda y seleccione **Soporte**.

   La página **Recursos** debería mostrar que su cuenta de consola está registrada para recibir soporte.

   Tenga en cuenta que otros usuarios de la consola no verán este mismo estado de registro de soporte si no han asociado una cuenta del sitio de soporte de NetApp con su inicio de sesión. Sin embargo, eso no significa que su cuenta no esté registrada para recibir soporte. Siempre que un usuario de la organización haya seguido estos pasos, su cuenta quedará registrada.

Soy cliente actual pero no tengo cuenta NSS

Si es un cliente existente de NetApp con licencias y números de serie existentes pero *no* una cuenta NSS, debe crear una cuenta NSS y asociarla con su inicio de sesión de la consola.

Pasos

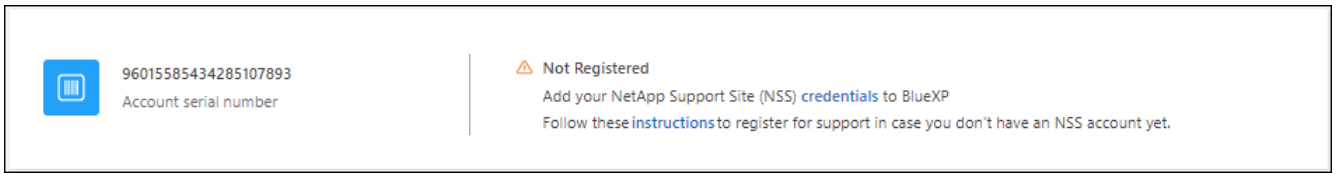
1. Cree una cuenta en el sitio de soporte de NetApp completando el "Formulario de registro de usuario del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
   b. Asegúrese de copiar el número de serie de la cuenta de la consola (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento de la cuenta.
2. Asocie su nueva cuenta NSS con su inicio de sesión de la consola completando los pasos a continuaciónCliente existente con una cuenta NSS .

Completamente nuevo en NetApp

Si es nuevo en NetApp y no tiene una cuenta NSS, siga cada paso a continuación.

Pasos

1. En la parte superior derecha de la Consola, seleccione el ícono Ayuda y seleccione **Soporte**.
2. Localice el número de serie de su ID de cuenta en la página de Registro de soporte.



3. Navegar a "Sitio de registro de soporte de NetApp" y seleccione *No soy un cliente registrado de NetApp *.
4. Llene los campos obligatorios (aquellos con asteriscos rojos).
5. En el campo **Línea de productos**, seleccione **Administrador de nube** y luego seleccione su proveedor de facturación correspondiente.
6. Copie el número de serie de su cuenta del paso 2 anterior, complete la verificación de seguridad y luego confirme que leyó la Política de privacidad de datos global de NetApp.

Se envía inmediatamente un correo electrónico al buzón proporcionado para finalizar esta transacción segura. Asegúrese de revisar sus carpetas de correo no deseado si el correo electrónico de validación no llega en unos minutos.

7. Confirme la acción desde el correo electrónico.

   Al confirmar, se envía su solicitud a NetApp y se recomienda que cree una cuenta en el sitio de soporte de NetApp .

8. Cree una cuenta en el sitio de soporte de NetApp completando el "Formulario de registro de usuario del sitio de soporte de NetApp"
   a. Asegúrese de seleccionar el nivel de usuario apropiado, que normalmente es **Cliente de NetApp /Usuario final**.
   b. Asegúrese de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente para el campo de número de serie. Esto acelerará el procesamiento.

Después de terminar

NetApp debería comunicarse con usted durante este proceso. Este es un ejercicio de incorporación único para nuevos usuarios.

Una vez que tenga su cuenta del sitio de soporte de NetApp , asocie la cuenta con su inicio de sesión de consola completando los pasos a continuación.Cliente existente con una cuenta NSS .

Asociar credenciales NSS para la compatibilidad con Cloud Volumes ONTAP

Es necesario asociar las credenciales del sitio de soporte de NetApp con su cuenta de consola para habilitar los siguientes flujos de trabajo clave para Cloud Volumes ONTAP:

- Registro de sistemas Cloud Volumes ONTAP de pago por uso para obtener soporte

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

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

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

- Actualización del software Cloud Volumes ONTAP a la última versión

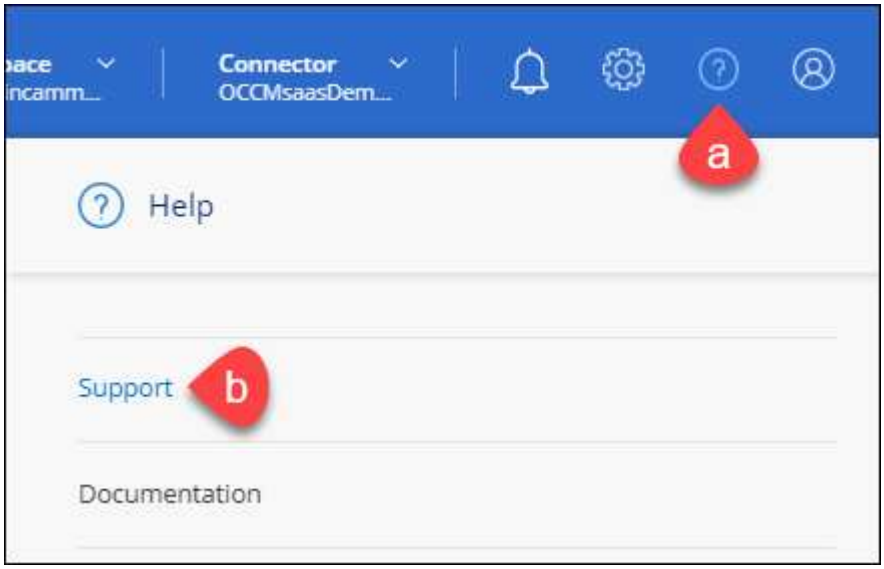
La asociación de credenciales NSS con su cuenta de NetApp Console es diferente a la asociación de una cuenta NSS con un inicio de sesión de usuario de consola.

Estas credenciales de NSS están asociadas con su ID de cuenta de consola específica. Los usuarios que pertenecen a la organización de la Consola pueden acceder a estas credenciales desde **Soporte > Administración de NSS**.

- Si tiene una cuenta de nivel de cliente, puede agregar una o más cuentas NSS.
- Si tiene una cuenta de socio o revendedor, puede agregar una o más cuentas NSS, pero no se pueden agregar junto con cuentas de nivel de cliente.

Pasos

1. En la parte superior derecha de la Consola, seleccione el ícono Ayuda y seleccione **Soporte**.



2. Seleccione **Administración de NSS > Agregar cuenta NSS**.
3. Cuando se le solicite, seleccione **Continuar** para ser redirigido a una página de inicio de sesión de Microsoft.

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

4. En la página de inicio de sesión, proporcione su dirección de correo electrónico y contraseña registradas en el sitio de soporte de NetApp para realizar el proceso de autenticación.

   Estas acciones permiten que la consola utilice su cuenta NSS para cosas como descargas de licencias, verificación de actualizaciones de software y futuros registros de soporte.

   Tenga en cuenta lo siguiente:

   - La cuenta NSS debe ser una cuenta de nivel de cliente (no una cuenta de invitado o temporal). Puede tener varias cuentas NSS a nivel de cliente.
   - Solo puede haber una cuenta NSS si esa cuenta es una cuenta de nivel de socio. Si intenta agregar cuentas NSS de nivel de cliente y existe una cuenta de nivel de socio, recibirá el siguiente mensaje de error:

     "El tipo de cliente NSS no está permitido para esta cuenta porque ya hay usuarios NSS de otro tipo".

   Lo mismo ocurre si tiene cuentas NSS de nivel de cliente preexistentes e intenta agregar una cuenta de nivel de socio.

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

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

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

     Al utilizar esta opción se le solicitará que inicie sesión nuevamente. Tenga en cuenta que el token de

estas cuentas caduca después de 90 días. Se publicará una notificación para avisarle de esto.

Obtener ayuda

NetApp proporciona soporte para NetApp Console y sus servicios en la nube de diversas maneras. Hay amplias opciones de autoayuda gratuitas disponibles las 24 horas del día, los 7 días de la semana, como artículos de la base de conocimientos (KB) y un foro comunitario. Su registro de soporte incluye soporte técnico remoto mediante tickets web.

Obtenga soporte para un servicio de archivos de un proveedor de nube

Para obtener soporte técnico relacionado con un servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que utilice el servicio, consulte la documentación de ese producto.

- "Amazon FSx para ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Para recibir soporte técnico específico para NetApp y sus soluciones de almacenamiento y servicios de datos, utilice las opciones de soporte que se describen a continuación.

Utilice opciones de autosuficiencia

Estas opciones están disponibles de forma gratuita, las 24 horas del día, los 7 días de la semana:

- Documentación

  La documentación de la NetApp Console que estás viendo actualmente.

- "Base de conocimientos"

  Busque en la base de conocimientos de NetApp para encontrar artículos útiles para solucionar problemas.

- "Comunidades"

  Únase a la comunidad de la NetApp Console para seguir las discusiones en curso o crear otras nuevas.

Cree un caso con el soporte de NetApp

Además de las opciones de autosoporte anteriores, puede trabajar con un especialista de soporte de NetApp para resolver cualquier problema después de activar el soporte.

Antes de empezar

- Para utilizar la función **Crear un caso**, primero debe asociar sus credenciales del sitio de soporte de NetApp con su inicio de sesión de la consola. "Aprenda a administrar las credenciales asociadas con su inicio de sesión en la consola" .
- Si está abriendo un caso para un sistema ONTAP que tiene un número de serie, entonces su cuenta NSS debe estar asociada con el número de serie de ese sistema.

Pasos

1. En la NetApp Console, seleccione **Ayuda > Soporte**.
2. En la página **Recursos**, elija una de las opciones disponibles en Soporte técnico:

   a. Seleccione **Llámenos** si desea hablar con alguien por teléfono. Serás dirigido a una página en netapp.com que enumera los números de teléfono a los que puedes llamar.

   b. Seleccione **Crear un caso** para abrir un ticket con un especialista de soporte de NetApp :

      - **Servicio**: Seleccione el servicio con el que está asociado el problema. Por ejemplo, * NetApp Console* cuando es específico de un problema de soporte técnico con flujos de trabajo o funcionalidad dentro de la consola.
      - **Sistema**: si corresponde al almacenamiento, seleccione * Cloud Volumes ONTAP* o **On-Prem** y luego el entorno de trabajo asociado.

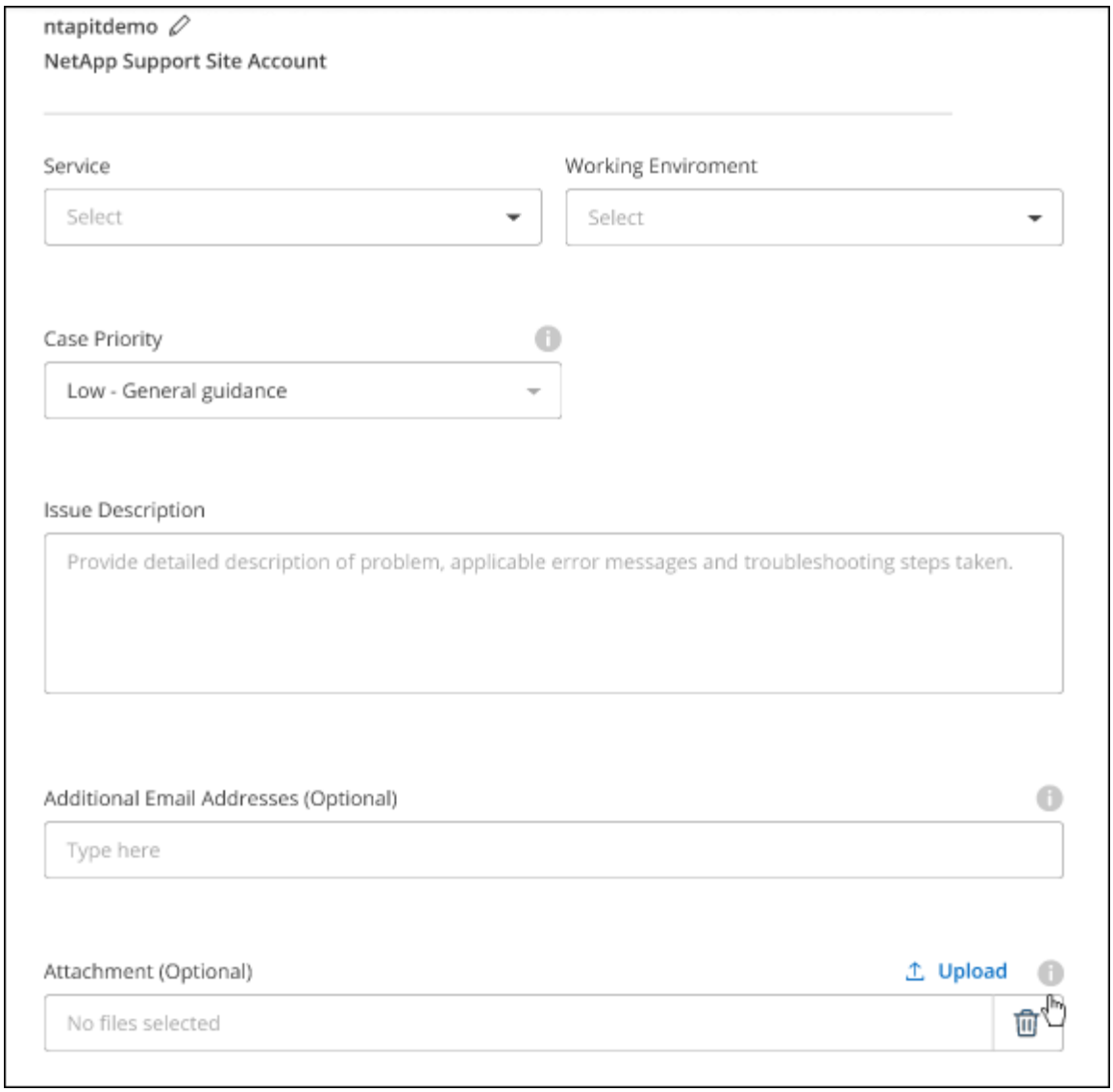
        La lista de sistemas está dentro del alcance de la organización de la consola y del agente de consola que ha seleccionado en el banner superior.

      - **Prioridad del caso**: elija la prioridad del caso, que puede ser Baja, Media, Alta o Crítica.

        Para obtener más detalles sobre estas prioridades, pase el mouse sobre el ícono de información junto al nombre del campo.

      - **Descripción del problema**: proporcione una descripción detallada de su problema, incluidos los mensajes de error aplicables o los pasos de solución de problemas que realizó.
      - **Direcciones de correo electrónico adicionales**: Ingrese direcciones de correo electrónico adicionales si desea informar a otra persona sobre este problema.
      - **Adjunto (opcional)**: cargue hasta cinco archivos adjuntos, uno a la vez.

        Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.



Después de terminar

Aparecerá una ventana emergente con su número de caso de soporte. Un especialista de soporte de NetApp revisará su caso y se comunicará con usted pronto.

Para obtener un historial de sus casos de soporte, puede seleccionar **Configuración > Cronología** y buscar acciones llamadas "crear caso de soporte". Un botón en el extremo derecho le permite ampliar la acción para ver detalles.

Es posible que encuentres el siguiente mensaje de error al intentar crear un caso:

"No está autorizado a crear un caso contra el servicio seleccionado"

Este error podría significar que la cuenta NSS y la empresa registrada con la que está asociada no son la misma empresa registrada para el número de serie de la cuenta de la NetApp Console (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puede buscar ayuda utilizando una de las siguientes opciones:

- Envíe un caso no técnico a https://mysupport.netapp.com/site/help

Gestione sus casos de soporte

Puede ver y administrar casos de soporte activos y resueltos directamente desde la Consola. Podrás gestionar los casos asociados a tu cuenta NSS y a tu empresa.

Tenga en cuenta lo siguiente:

- El panel de gestión de casos en la parte superior de la página ofrece dos vistas:
  - La vista de la izquierda muestra el total de casos abiertos en los últimos 3 meses por la cuenta de usuario NSS que usted proporcionó.
  - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de su empresa en función de su cuenta de usuario NSS.

  Los resultados en la tabla reflejan los casos relacionados con la vista que usted seleccionó.
- Puede agregar o eliminar columnas de interés y puede filtrar el contenido de columnas como Prioridad y Estado. Otras columnas sólo proporcionan capacidades de clasificación.

  Vea los pasos a continuación para obtener más detalles.
- A nivel de caso, ofrecemos la posibilidad de actualizar notas de caso o cerrar un caso que aún no esté en estado Cerrado o Pendiente de cierre.

Pasos

1. En la NetApp Console, seleccione **Ayuda > Soporte**.
2. Seleccione **Administración de casos** y, si se le solicita, agregue su cuenta NSS a la consola.

   La página **Administración de casos** muestra los casos abiertos relacionados con la cuenta NSS que está asociada con su cuenta de usuario de la consola. Esta es la misma cuenta NSS que aparece en la parte superior de la página de **administración de NSS**.
3. Modifique opcionalmente la información que se muestra en la tabla:
   - En **Casos de la organización**, seleccione **Ver** para ver todos los casos asociados a su empresa.
   - Modifique el rango de fechas eligiendo un rango de fechas exacto o eligiendo un período de tiempo diferente.
   - Filtrar el contenido de las columnas.
   - Cambie las columnas que aparecen en la tabla seleccionando y luego elegir las columnas que desea mostrar.
4. Gestionar un caso existente seleccionando y seleccionando una de las opciones disponibles:
   - **Ver caso**: Ver detalles completos sobre un caso específico.
   - **Actualizar notas del caso**: proporcione detalles adicionales sobre su problema o seleccione **Cargar archivos** para adjuntar hasta un máximo de cinco archivos.

     Los archivos adjuntos están limitados a 25 MB por archivo. Se admiten las siguientes extensiones de archivo: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx y csv.
   - **Cerrar caso**: proporcione detalles sobre el motivo por el cual está cerrando el caso y seleccione **Cerrar caso**.

Avisos legales

Los avisos legales proporcionan acceso a declaraciones de derechos de autor, marcas comerciales, patentes y más.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marcas comerciales

NETAPP, el logotipo de NETAPP y las marcas enumeradas en la página de Marcas comerciales de NetApp son marcas comerciales de NetApp, Inc. Otros nombres de empresas y productos pueden ser marcas comerciales de sus respectivos propietarios.

"https://www.netapp.com/company/legal/trademarks/"

Patentes

Puede encontrar una lista actualizada de las patentes propiedad de NetApp en:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Política de privacidad

"https://www.netapp.com/company/legal/privacy-policy/"

Código abierto

Los archivos de aviso proporcionan información sobre derechos de autor y licencias de terceros utilizados en el software de NetApp .

"Aviso para la NetApp Console"

Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

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

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

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

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

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

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

Información de la marca comercial

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