Instala y configura

NetApp Console local deployment

NetApp
August 10, 2026

Tabla de contenidos

Instala y configura

Guía de inicio rápido para configurar la implementación local de la consola NetApp Console

Después de instalar NetApp Console local deployment, configura tu organización para que los equipos adecuados puedan gestionar de forma segura los recursos de almacenamiento correctos. Usa esta lista de comprobación para planificar tu estructura, organizar recursos, añadir miembros, configurar integraciones y habilitar servicios de datos.

Roles de acceso necesarios

Superadministrador o administrador de la organización. "Conoce los roles de acceso".

1 Instala la implementación local de NetApp Console

- Revisa el flujo de trabajo de instalación para comprender el proceso de implementación. "Conoce el flujo de instalación para la implementación local de NetApp Console".
- Instala NetApp Console local deployment en tu vCenter. "Instala la implementación local de NetApp Console".

2 Planifica tu organización

- Descubre cómo las carpetas y las flotas te ayudan a organizar tus recursos. "Conoce las carpetas y flotas".
- Descubre cómo el control de acceso basado en roles (RBAC) concede a los miembros el acceso que necesitan. "Conoce el control de acceso basado en roles en la implementación local de NetApp Console".
- Revisa el flujo de trabajo de gestión de identidades y accesos. "Empieza a utilizar IAM para la gestión de flotas y gestión de recursos".

3 Configura tu organización

- Agrega tus sistemas de almacenamiento a la implementación local de NetApp Console. "Agregar sistemas de almacenamiento".
- Crea la jerarquía de carpetas y flotas que se ajuste a la estructura de tu empresa. "Crear carpetas y flotas".
- Asocia los recursos con las carpetas y flotas correctas. "Asocia recursos a carpetas y flotas".
- Agrega miembros y asígnales sus roles iniciales. "Agregar miembros y asignar roles".

4 Configura integraciones y servicios

- Integra con Active Directory para que los usuarios del directorio puedan acceder a la implementación local de la NetApp Console. "Integra con Active Directory".
- Conecta tu modelo de lenguaje a gran escala (LLM) para activar el asistente de la consola y la gestión

asistida por IA. "Conecta tu LLM".

- Configura cómo la implementación local de la NetApp Console entrega las notificaciones. "Configura la entrega de notificaciones".

5 **Configura NetApp Backup and Recovery**

- "Obtén una licencia para NetApp Backup and Recovery". Puedes saltarte este paso si no quieres acceder a los servicios avanzados de NetApp Backup and Recovery.
- Agrega la licencia de NetApp Backup and Recovery al despliegue local de NetApp Console. "Agrega la licencia a la implementación local de NetApp Console".
- "Concede a los usuarios acceso a NetApp Backup and Recovery".

Instala NetApp Console

Instala el despliegue local de NetApp Console mediante una OVA en vCenter

Usas un archivo OVA para instalar una implementación local de NetApp Console en tu vCenter. La descarga del OVA o la URL están disponibles en el sitio de soporte de NetApp.

Prepárate para instalar la implementación local de NetApp Console

Antes de la instalación, asegúrate de que tu host de máquinas virtuales cumpla los requisitos y de que la implementación local de la NetApp Console pueda acceder a internet y a las redes de destino. Para usar los servicios de datos de NetApp como NetApp Backup and Recovery, crea credenciales de proveedor de nube para que la implementación local de la NetApp Console pueda realizar acciones en tu nombre.

Revisa los requisitos del host para la implementación local de NetApp Console

Asegúrate de que tu equipo host cumpla los requisitos de instalación antes de instalar NetApp Console en una implementación local.

- CPU: 16 núcleos o 16 vCPUs
- RAM: 64 GB
- Espacio en disco: 596 GB (se recomienda el aprovisionamiento completo)
- vSphere 7.0u3 o superior, con hardware virtual versión 19 o superior

> Instala NetApp Console local deployment en un entorno vCenter en lugar de directamente en un host ESXi.

Configura el acceso a la red para la implementación local de la NetApp Console

NetApp Console local deployment utiliza un espacio de direcciones fijo para la comunicación entre servicios. El rango de direcciones IP 10.42.0.0/16 y 10.43.0.0/16 se usa para la red interna. Antes de implementar Console local deployment, asegúrate de que estos rangos de IP no estén asignados a otras instancias de VM, ámbitos DHCP, registros DNS o grupos VIP del balanceador de carga en las VLAN disponibles para Console local deployment.

Consulta el artículo de base de conocimientos Agent IP conflict with existing network para obtener

instrucciones sobre cómo cambiar la dirección IP de las interfaces del agente.

Instala la implementación local de NetApp Console en tu entorno de vCenter

NetApp permite instalar NetApp Console local deployment en tu entorno vCenter. El archivo OVA incluye una imagen de máquina virtual preconfigurada que puedes implementar en tu entorno VMware.

Descarga el OVA o copia la URL

Descarga el OVA.

1. Descarga el software de implementación local de Console desde el sitio de soporte de NetApp.

Implementa NetApp Console de forma local en tu vCenter

Inicia sesión en tu entorno de vCenter para implementar la instalación local de Console.

Pasos

1. Sube el certificado autofirmado a tu lista de certificados de confianza si tu entorno lo requiere. Puedes sustituir este certificado tras la instalación.
2. Implementa el archivo OVA desde la biblioteca de contenidos o desde el sistema local.

Desde el sistema local	De la biblioteca de contenidos
a. Haz clic con el botón derecho y selecciona **Implementar plantilla OVF…**. b. Elige el archivo OVA desde la URL o busca su ubicación, luego selecciona **Siguiente**.	a. Ve a tu biblioteca de contenidos y selecciona el OVA de la consola. b. Selecciona **Acciones** > **Nueva máquina virtual a partir de esta plantilla**

3. Completa el asistente «Implementar plantilla OVF» para implementar la Console.
4. Selecciona un nombre y una carpeta para la máquina virtual, luego selecciona **Siguiente**.
5. Selecciona un recurso de computación y luego selecciona **Siguiente**.
6. Revisa los detalles de la plantilla y, a continuación, selecciona **Siguiente**.
7. Acepta el contrato de licencia y luego selecciona **Siguiente**.
8. Elige el tipo de configuración de proxy que deseas utilizar: proxy explícito, proxy transparente o sin proxy.
9. Selecciona el almacén de datos donde quieres implementar la máquina virtual y luego selecciona **Siguiente**. Asegúrate de que cumple los requisitos del host.
10. Selecciona la red a la que quieres conectar la VM y luego selecciona **Siguiente**. Asegúrate de que la red sea IPv4 y tenga acceso a internet de salida a los endpoints requeridos.
11. En la ventana **Personalizar plantilla**, rellena los siguientes campos:
    - **Información del proxy**
      - Si seleccionaste proxy explícito, introduce 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 seleccionaste el proxy transparente, sube el certificado correspondiente.
    - **Configuración de la máquina virtual**
      - **Omitir comprobación de configuración**: Esta casilla de comprobación viene desmarcada por defecto, lo que significa que la implementación local de la NetApp Console ejecuta una comprobación de configuración para validar el acceso a la red.

- NetApp recomienda dejar esta casilla de comprobación sin marcar para que la instalación incluya una comprobación de la configuración de la implementación local de la NetApp Console. La comprobación de configuración verifica que la implementación local de la NetApp Console tenga acceso de red a los endpoints requeridos. Si la implementación falla debido a problemas de conectividad, puedes acceder al informe de validación y a los registros desde el host de la implementación local de la NetApp Console. En algunos casos, si estás seguro de que la implementación local de la NetApp Console tiene acceso a la red, puedes optar por omitir la comprobación.

- **Contraseña de mantenimiento**: Establece la contraseña para el usuario `maint` que permite acceder a la consola de mantenimiento de la implementación local de NetApp Console.
- **Servidores NTP**: Indica uno o varios servidores NTP para la sincronización horaria.
- **Nombre de host**: Establece el nombre de host de esta VM. No debe incluir el dominio de búsqueda. Por ejemplo, un FQDN como console10.searchdomain.company.com debe introducirse como console10.
- **DNS principal**: Indica el servidor DNS principal que se utilizará para la resolución de nombres.
- **DNS secundario**: Indica el servidor DNS secundario que se utilizará para la resolución de nombres.
- Dominios de búsqueda: Especifica el nombre de dominio de búsqueda que se debe usar al resolver el nombre de host. Por ejemplo, si el FQDN es console10.searchdomain.company.com, introduce searchdomain.company.com.
- **Dirección IPv4**: la dirección IP asociada al nombre de host.
- **Máscara de subred IPv4**: la máscara de subred de la dirección IPv4.
- **Dirección de la puerta de enlace IPv4**: La dirección de la puerta de enlace para la dirección IPv4.

12. Selecciona **Siguiente**.
13. Revisa los detalles en la ventana **Listo para finalizar** y selecciona **Finalizar**.

    La barra de tareas de vSphere muestra el progreso a medida que se implementa la implementación local de NetApp Console.

14. Enciende la máquina virtual.

Planifica tu organización de la consola

Comienza con la gestión de identidades y accesos en la implementación local de NetApp Console

En una implementación local de NetApp Console, configura la jerarquía de carpetas y flotas, añade miembros y permisos iniciales, y añade y coloca los recursos en las flotas correctas para que los equipos adecuados puedan acceder a ellos y gestionarlos.

Roles de acceso necesarios

Superadministrador, administrador de la organización o administrador de carpetas o flotas. "Conoce los roles de acceso".

Necesitas el rol de **Organization admin** o **Super admin** para completar la configuración inicial. Después de la configuración, gestiona los recursos, el acceso de los miembros y el acceso a la flota a medida que tu organización cambie.

Agrega o descubre recursos

Agrega sistemas a la implementación local de Console. Durante la configuración inicial, los sistemas suelen añadirse mientras la flota predeterminada está seleccionada.

Aprende a crear o descubrir recursos:

- "Clústeres de ONTAP locales"

Crea tu jerarquía de carpetas y flotas

Crea flotas y carpetas adicionales que se ajusten a la jerarquía de tu empresa.

"Descubre cómo organizar tus recursos con carpetas y flotas".

Asocia los recursos con las flotas correctas

Al añadir o descubrir un sistema en la implementación local de Console, el recurso se asocia automáticamente a la flota seleccionada en ese momento. Para que un sistema esté disponible para los equipos adecuados, asócialo a las flotas correspondientes de tu jerarquía.

- "Aprende a gestionar los recursos en carpetas y flotas".

Agrega miembros y asigna permisos iniciales

Añade miembros y asígnales funciones a nivel de organización, carpeta o flota según lo que gestionen.

"Aprende a gestionar los miembros y sus permisos".

Tras la configuración inicial

Después de completar la configuración inicial, gestiona el acceso y la asignación de recursos a medida que tu organización cambie:

- "Gestiona los recursos en carpetas y flotas"
- "Gestiona el acceso de los miembros en todas las flotas y carpetas (centrado en los miembros)"
- "Gestiona quién puede acceder a una flota o carpeta específica (centrado en la flota)"
- "Elimina las carpetas y las flotas cuando ya no las necesites"

Información relacionada

- "Aprende sobre la gestión de identidades y accesos en NetApp Console"
- "Conoce la API de identidad y acceso"

Conoce las carpetas y las flotas en la implementación local de NetApp Console

En una implementación local de NetApp Console, utiliza carpetas y flotas de almacenamiento para organizar tus recursos de NetApp y controlar el acceso según tu estructura empresarial: por ubicación, departamento o tipo de carga de trabajo.

Utiliza esta página para consultar la estrategia de jerarquía y los patrones de diseño de flotas. Para ver un modelo completo de IAM con miembros, roles y ámbito de recursos, consulta "Infórmate sobre la gestión de identidades y accesos en la implementación local de NetApp Console".

Organizas los recursos en una jerarquía: la organización está en la parte superior, luego las carpetas (que pueden contener otras carpetas o flotas) y después las flotas, que contienen los sistemas de almacenamiento. Asigna roles de acceso en el nivel de organización, carpeta o flota para que los usuarios tengan el acceso adecuado a los recursos.

Debes tener el rol de administrador de la organización o el de administrador de carpetas o flotas para gestionar carpetas y flotas en la implementación local de la NetApp Console.

Componentes organizativos

Los componentes organizativos —la organización, las carpetas y las flotas— forman una jerarquía que determina cómo se agrupan los recursos y cómo se delega el acceso.

Organización

Una organización es el nivel superior de la jerarquía de implementación local de la NetApp Console y normalmente representa tu empresa. Tu organización está formada por carpetas, flotas, miembros, roles y recursos. Los recursos están asociados a flotas y los miembros reciben roles en el nivel de organización, carpeta o flota.

Carpetas

Las carpetas agrupan flotas relacionadas para organizarlas por ubicación, centro o unidad de negocio. No puedes asociar sistemas de almacenamiento directamente con carpetas, pero asignar a un miembro un rol a nivel de carpeta le da acceso a todas las flotas en esa carpeta.

Los administradores de la organización pueden añadir un recurso a una carpeta para delegar la tarea de asociar dicho recurso a las flotas a un administrador de la carpeta o de la flota. "Asocia recursos con carpetas y flotas".

Flotas

Sistemas de almacenamiento agrupados por flotas. Asigna recursos a las flotas y concede acceso a los miembros a nivel de flota. Los recursos pueden pertenecer a varias flotas. Los miembros con acceso a una flota pueden gestionar los recursos de esa flota.

Por ejemplo, puedes asociar un sistema ONTAP local a una sola flota o a todas las flotas de tu organización, según tus necesidades.

"Aprende a crear carpetas y flotas de almacenamiento".

Recursos

Un recurso es un sistema de almacenamiento que la implementación local de Console reconoce y que puede asignarse a una flota. Asocia un recurso a una flota para que los usuarios con acceso a la flota puedan gestionar dicho recurso.

Por ejemplo, puedes asociar un clúster ONTAP a una flota o a todas las flotas de tu organización. La forma de asociar un recurso depende de las necesidades de tu organización.

"Aprende a asociar recursos a flotas".

Miembros y funciones

Los miembros son los usuarios y las cuentas de servicio de tu organización. Los roles definen qué acciones pueden realizar y en qué nivel de la jerarquía: organización, carpeta o flota.

Miembros

Los miembros de tu organización son cuentas de usuario o cuentas de servicio. Una cuenta de servicio normalmente la usa una aplicación para completar tareas específicas sin intervención humana.

Los usuarios con el rol de administrador de la organización pueden añadir nuevos miembros a tu organización. Todos los usuarios (incluidas las cuentas de servicio y los usuarios de Active Directory) deben añadirse explícitamente y se les debe asignar al menos un rol para que puedan acceder a la implementación local de Console.

"Descubre cómo añadir miembros a tu organización".

Roles de acceso

La implementación local de Console ofrece roles de acceso que puedes asignar a los miembros de tu organización.

Al asignar un miembro a un rol, puedes conceder dicho rol a toda la organización, a una carpeta concreta o a una flota específica. El rol que selecciones otorga al miembro permiso para los recursos en la parte seleccionada de la jerarquía.

La implementación local de la NetApp Console ofrece roles detallados que se ajustan al principio del mínimo privilegio, lo que significa que los roles de acceso están diseñados para que los usuarios solo tengan acceso a lo que necesitan.

Los usuarios pueden desempeñar varias funciones a medida que se amplían sus responsabilidades.

Herencia de roles

Cuando asignas un rol a nivel de organización o de carpeta, las subcarpetas, flotas y recursos que se encuentran por debajo de ella heredan ese rol, por lo que el diseño de tus carpetas y flotas determina el alcance de cada asignación.

"Conoce la herencia de roles en la implementación local de NetApp Console".

Ejemplos de diseño organizativo

La estructura organizativa adecuada depende del tamaño de tu organización y de cómo estén organizados tus equipos. Los siguientes ejemplos muestran cómo diferentes organizaciones pueden utilizar la jerarquía de carpetas y flotas para gestionar el acceso de forma eficaz.

Estrategia para pequeñas organizaciones

Para organizaciones con menos de 50 usuarios y gestión centralizada del almacenamiento, considera un enfoque simplificado usando los roles de Super admin y Super viewer.

Ejemplo: ABC Corporation (equipo de 5 personas)

- **Estructura**: Una única organización con 3 flotas (Producción, Desarrollo, Backup)
- **Roles**:
  - 2 miembros sénior: rol de super admin para acceso administrativo completo

    - 3 miembros del equipo: rol de super viewer para la supervisión sin derechos de modificación
- **Ventajas**: gestión simplificada, menor complejidad de los roles, adecuado para equipos que necesitan un amplio acceso

Estrategia empresarial multirregional

Para las grandes organizaciones con operaciones regionales y equipos especializados, implementa un enfoque jerárquico con carpetas que representen los límites geográficos o de las unidades de negocio.

Ejemplo: XYZ Corporation (empresa multinacional)

- **Estructura**: Organización > Carpetas regionales (América del Norte, Europa, Asia-Pacífico) > Flotas por región
- **Funciones de la plataforma**:
    - 1 Administrador de la organización: supervisión global y gestión de políticas
    - 3 administradores de carpetas o de flotas: control regional (uno por región)
    - 1 Federación admin: integración del servicio de directorio corporativo
- **Funciones de almacenamiento por región**:
    - Administrador de almacenamiento: descubre y gestiona los sistemas de almacenamiento en las regiones asignadas
    - Visor de almacenamiento: supervisa los recursos de almacenamiento en todas las regiones
    - Especialista en estado del sistema: gestiona el estado del almacenamiento sin necesidad de realizar modificaciones en el sistema
- **Ventajas**: mayor seguridad gracias a la separación de funciones, la autonomía regional y el cumplimiento de la normativa local

Estrategia de especialización departamental

Para las organizaciones con equipos especializados que requieren un acceso específico, usa asignaciones de roles específicas basadas en responsabilidades funcionales.

Ejemplo: TechCorp (empresa tecnológica de tamaño medio)

- **Estructura**: Organización > Carpetas de departamento (TI, Seguridad, Desarrollo) > Recursos específicos de la flota
- **Funciones especializadas**:
    - Equipo de seguridad: roles de administrador de resiliencia ante el ransomware y visor de clasificaciones
    - Equipo de copias de seguridad: superadministrador de copias de seguridad y recuperación para operaciones integrales de copias de seguridad
    - Equipo de desarrollo: administrador de almacenamiento para la gestión del entorno de prueba
    - Equipo de cumplimiento normativo: analista de apoyo operativo para la supervisión y la gestión de casos de asistencia
- **Ventajas**: control de acceso personalizado, mayor eficiencia operativa y una clara asignación de responsabilidades en tareas especializadas

Próximos pasos

- "Crear carpetas y flotas de almacenamiento"
- "Asocia recursos con carpetas y flotas"
- "Gestiona las asignaciones de acceso a la flota"
- "Supervisar o auditar las acciones de implementación local de Console"

Conoce el control de acceso basado en roles en la implementación local de NetApp Console

Gestiona el acceso de los usuarios a la implementación local de NetApp Console mediante el control de acceso basado en roles (RBAC), asignando roles predefinidos a nivel de organización, carpeta o flota. Cada rol otorga permisos específicos que definen qué acciones pueden realizar los usuarios dentro del ámbito que se les ha asignado.

NetApp diseña los roles de implementación local de Console siguiendo el principio de menor privilegio, así 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 flotas, asigna a los miembros de la organización uno o varios roles para carpetas o flotas específicas, que les permitan realizar solo sus responsabilidades.

Por ejemplo, puedes asignar a un miembro el rol de Backup and Recovery admin para un nivel de flota específico, permitiéndole realizar operaciones de Backup and Recovery en los recursos dentro de esa flota, sin darle acceso más amplio a toda la organización. A este mismo usuario puedes asignarle el rol para varias flotas dentro de tu organización.

Puedes asignar a los miembros varios roles para el mismo ámbito o para ámbitos diferentes, en función de sus responsabilidades. Por ejemplo, una organización más pequeña podría asignar al mismo miembro los roles de Storage admin y Backup and Recovery admin a nivel de organización, mientras que una organización más grande podría tener diferentes miembros asignados a cada rol a nivel de flota.

Tipos de miembros de la organización de la consola

NetApp Console la implementación local admite los siguientes tipos de miembros:

- *Usuarios*: Los usuarios individuales pueden ser usuarios locales que añadas a NetApp Console local deployment y que utilicen credenciales locales, o bien usuarios de directorio que se autentiquen a través de tu servicio integrado de Active Directory o LDAP. A ambos tipos de usuarios se les pueden asignar roles en NetApp Console local deployment para acceder a los recursos.
- *Cuentas de servicio*: Cuentas no humanas que utilizan las aplicaciones o los servicios para interactuar con NetApp Console implementación local a través de las API. Puedes añadir cuentas de servicio directamente a tu organización de implementación local de Console.

"Descubre cómo añadir miembros a tu organización."

Roles predefinidos en la implementación local de NetApp Console

La implementación local de 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 flota).

NetApp Console los roles de implementación local usan principios de privilegio mínimo que aseguran que los miembros solo tengan los permisos necesarios para sus tareas y categorizan los roles según el tipo de acceso que proporcionan:

- Funciones de la plataforma: otorga permisos de administración para la implementación local de Console
- Roles de servicios de datos: Otorgan permisos para gestionar servicios de datos específicos, como Ransomware Resilience y Backup and Recovery
- Funciones de la aplicación: otorgan permisos para gestionar el almacenamiento, así como para auditar los eventos y alertas de la implementación local de la consola

Puedes asignar varios roles a un miembro en función de sus responsabilidades. Por ejemplo, podrías asignar a un miembro tanto el rol de Storage admin como el de Backup and Recovery admin para una flota concreta.

Para elegir el acceso de un miembro, haz coincidir la categoría del rol con las responsabilidades del miembro y luego asigna el rol en el ámbito (organización, carpeta o flota) que corresponda a lo amplio que debe ser ese acceso para el miembro. "Descubre cómo diferentes organizaciones estructuran los roles y el alcance en NetApp Console implementación local".

"Infórmate sobre los roles predefinidos que puedes asignar a los miembros en NetApp Console implementación local".

Cómo funciona la herencia de roles

Cuando asignas un rol a nivel de organización o de carpeta, ese rol se hereda en los ámbitos subordinados dentro de esa parte de la jerarquía. Esto significa que los roles a nivel de organización se aplican en toda la organización, los roles a nivel de carpeta se aplican a todas las carpetas subordinadas y flotas de esa carpeta, y los roles a nivel de flota se aplican solo a los recursos de esa flota.

Utiliza el ámbito que se ajuste al acceso que deseas que tenga el miembro. Por ejemplo, asigna un rol a nivel de carpeta cuando el miembro necesite el mismo acceso en varias flotas de una misma región. Asigna el rol a nivel de flota cuando el miembro deba acceder únicamente a una flota.

No puedes anular el acceso heredado en un ámbito inferior. Si un miembro hereda un rol de la organización o de una carpeta, cambia esa asignación en el ámbito superior donde la concediste originalmente.

"Conoce las carpetas y las flotas en la implementación local de NetApp Console". "Gestiona el acceso de los miembros". "Gestiona las asignaciones de acceso a la flota".

Configura tu organización en Console

Agrega carpetas y flotas a tu organización de implementación local de NetApp Console

Crea carpetas y flotas que se adapten a la estructura de tu empresa, controla el acceso y organiza los recursos en NetApp Console implementación local.

Roles de acceso necesarios

Superadministrador, administrador de la organización o administrador de carpetas o flotas. "Conoce los roles de acceso".

La implementación local de NetApp Console crea una flota predeterminada cuando creas una organización. Puedes añadir más flotas y agruparlas en carpetas. "Conoce la jerarquía de recursos en NetApp Console".

Uso de carpetas y flotas para organizar los recursos

Las carpetas y las flotas son los dos pilares fundamentales que te permiten adaptar tu organización para que se ajuste a la forma en que trabajan realmente tus equipos. Por ejemplo, una carpeta por región con una flota de producción y una de desarrollo dentro de cada una.

- Las carpetas agrupan flotas relacionadas y permiten la administración delegada y la herencia de roles.
- Las flotas son donde asocias recursos para la gestión y donde das acceso operativo a los usuarios.

Puedes crear primero carpetas y flotas y añadir recursos y acceso de los miembros más adelante. Esto te permite planificar la jerarquía de recursos antes de añadir usuarios y recursos en la implementación local de NetApp Console. Si ya tienes definida la estructura, puedes añadir recursos y asignar acceso cuando crees la flota. Puedes actualizar las flotas en cualquier momento.

Por ejemplo, pon los clústeres de producción en una flota de producción y los clústeres de prueba en una flota de prueba, y da a cada equipo acceso solo a la flota que le pertenece.

Carpetas

Las carpetas organizan las flotas según la estructura de la empresa, como por unidad de negocio, región o equipo. Puedes anidar carpetas para reflejar tu organización.

Los roles asignados a nivel de carpeta se heredan en las carpetas secundarias y las flotas. También puedes usar una carpeta para delegar las tareas de asignación de flotas a un administrador de carpeta o de flota para esa parte de la jerarquía.

> Los miembros trabajan con flotas, no con carpetas. Un recurso asociado únicamente a una carpeta no puede ser gestionado por los miembros hasta que se asocie a una flota.

Por ejemplo, una empresa regional podría utilizar carpetas para organizar el almacenamiento ONTAP por unidad de negocio y carga de trabajo. Podría crear una carpeta de nivel superior para North America, subcarpetas para Production y Development, y flotas para los clústeres ONTAP que alojan SAP, VMware y volúmenes de backup. Los administradores de almacenamiento asignados a la carpeta de North America heredan el acceso a todas las flotas secundarias, mientras que los equipos de aplicaciones solo tienen acceso a las flotas que gestionan.

Flotas

Asocia recursos con las flotas para que los miembros puedan gestionarlos. Una flota puede existir directamente bajo la organización o dentro de una carpeta.

Por ejemplo, una empresa del sector sanitario utiliza el almacenamiento ONTAP en flotas independientes de producción y desarrollo. La flota de producción ejecuta aplicaciones clínicas y bases de datos de historiales de pacientes, mientras que la flota de desarrollo se encarga de las pruebas y la validación. Esta separación protege los datos activos, impone un control de acceso más estricto a la producción, facilita la auditabilidad y los controles de privilegios mínimos, y permite a los equipos de desarrollo trabajar sin afectar las cargas de trabajo orientadas a los pacientes.

Los usuarios navegan entre las flotas asignadas en la página **Sistemas** para gestionar los recursos asociados a cada flota.

Agrega una carpeta o fleet

Añade una flota siempre que necesites un nuevo límite para los recursos y el acceso de los miembros, y

añade una carpeta cuando quieras agrupar flotas relacionadas y delegar su administración. Por ejemplo, añade una `Production` carpeta que contenga una `Production-US-East` flota y una `Production-EU-West` flota, luego asigna a un responsable regional el rol de administrador de carpeta o de flota solo en su propia flota.

Puedes crear hasta siete niveles jerárquicos.

Puedes añadir recursos y asignar acceso a los miembros cuando creas una flota o una carpeta, o puedes hacerlo más tarde.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Organization**.
3. En la página **Organización**, selecciona **Add folder or fleet**.
4. Selecciona **Carpeta** o **Flota**.
5. En **Nombre y ubicación**: introduce un nombre y elige una ubicación para la carpeta o la flota.

1. Opcional: despliega la sección **Recursos** para asociar recursos a la flota o a la carpeta.
   a. Marca la casilla de comprobación situada junto al recurso que quieras asociar y luego selecciona **Asociar a la flota**. Si aún no has añadido sistemas a Console local deployment, puedes hacer este paso más tarde.

   > Los miembros no pueden acceder a los recursos de una carpeta hasta que esos recursos se asignen a una flota.

2. Opcional: despliega la sección **Acceso** para asignar acceso a los miembros. Selecciona **Add a member** para asignar acceso y un rol. Por defecto, el usuario que crea la flota tiene acceso a ella.

   "Conoce los roles de acceso".

3. Selecciona **Add**.

Cambiar el nombre de una carpeta o flota

Cambia el nombre de una carpeta o flota según sea necesario. Cambiar el nombre no afecta a los recursos asociados ni al acceso de los miembros.

Pasos

1. Desde la página **Organización**, ve a una flota o carpeta de la tabla, selecciona ••• y luego selecciona **Editar carpeta** o **Editar flota**.
2. En la página **Editar**, introduce un nuevo nombre y selecciona **Aplicar**.

Eliminar una carpeta o flota

Elimina las carpetas y flotas que ya no necesites, como después de una reestructuración del equipo o al completar una flota.

Antes de eliminar una carpeta o una flota, completa las siguientes comprobaciones:

- Comprueba que la carpeta o la flota no contengan recursos. "Descubre cómo eliminar las asociaciones de recursos".

- Comprueba qué miembros siguen teniendo acceso a la carpeta o a la flota. "Ver asignaciones de acceso de los miembros".
- Elimina o actualiza los permisos de acceso de los miembros según sea necesario. "Modificar las asignaciones de acceso de los miembros".
- Si vas a eliminar una flota, traslada primero los recursos a la flota de destino. "Descubre cómo trasladar recursos entre flotas".

Pasos

1. Desde la página **Organización**, ve a una flota o carpeta de la tabla, selecciona ••• y luego selecciona **Eliminar**.
2. Confirma que deseas eliminar la carpeta o la flota.

Gestiona flotas y carpetas en la implementación local de NetApp Console

Después de la configuración inicial, puedes hacer lo siguiente:

- **Gestiona las asociaciones de recursos para carpetas y flotas**: "Aprende a asociar recursos a flotas y carpetas".
- **Ver o actualizar los permisos de acceso a una carpeta o a una flota**: "Descubre cómo conceder acceso a las flotas a los usuarios".
- **Gestiona un miembro en varias carpetas y flotas**: "Aprende a gestionar el acceso de los miembros".
- **Añade miembros adicionales y asigna permisos iniciales**: "Aprende a gestionar los miembros y los permisos".

Información relacionada

- "Conoce la identidad y el acceso en NetApp Console"
- "Empieza con la identidad y el acceso en NetApp Console"
- "Gestiona las asignaciones de acceso a la flota"
- "Conoce la API de identidad y acceso"

Agrega sistemas de almacenamiento a la implementación local de NetApp Console

Añade sistemas de almacenamiento a la implementación local de NetApp Console para habilitar la supervisión, la gestión de inventario y la administración de tu infraestructura de almacenamiento. Una vez añadido un sistema de almacenamiento, la implementación local de Console detecta el sistema y comienza a recopilar información que puede utilizarse para tareas de supervisión y gestión.

Antes de empezar, asegúrate de que tienes los permisos necesarios para añadir sistemas de almacenamiento y de que el sistema de almacenamiento sea accesible desde la implementación local de Console.

Pasos

1. Selecciona **Storage > Management**.
2. En la lista desplegable «Ámbito», selecciona la flota a la que quieres añadir un sistema de almacenamiento.
3. Selecciona **Add system**.

4. Introduce los datos necesarios del sistema de almacenamiento, incluida la información de conexión y las credenciales.
5. Revisa la información que has introducido y selecciona **Add**.

   El sistema de almacenamiento se añade a la flota seleccionada. La implementación local de la consola comienza a detectar y supervisar el sistema. Dependiendo del entorno y la conectividad de red, puede tardar varios minutos en que el sistema aparezca como totalmente gestionado.

> También puedes añadir un sistema de almacenamiento desde la página **Administración > Identidad y acceso** seleccionando **Añadir sistema** e introduciendo la información necesaria sobre el sistema.

Administra recursos en carpetas y flotas en la implementación local de NetApp Console

Gestiona el acceso a los recursos en la implementación local de NetApp Console asociando los recursos con la carpeta o flota correcta, lo que controla qué equipos pueden acceder y gestionarlos.

Roles de acceso necesarios

Superadministrador, administrador de la organización o administrador de carpetas o flotas. "Conoce los roles de acceso".

Coloca los recursos donde los equipos adecuados puedan gestionarlos, muévelos cuando cambie la titularidad y elimina las asociaciones cuando ya no sean necesarias.

Un *recurso* es una entidad que reconoce la implementación local de Console, como un recurso de almacenamiento o una carga de trabajo de Backup and Recovery.

Tipos de recursos de la consola

La implementación local de la consola es compatible tanto con recursos de almacenamiento como con cargas de trabajo de Backup and Recovery. Asocia cualquiera de los dos tipos de recursos a una flota para controlar el acceso y la gestión.

Recursos de almacenamiento

Los recursos de almacenamiento son el tipo de recurso más habitual en tu organización. Cuando añadas un sistema de almacenamiento a una implementación local de Console, asócialo a una flota para que los equipos correspondientes puedan acceder a él y gestionarlo. Por ejemplo, tras añadir un clúster ONTAP, asócialo a la `Production-US-East` flota.

Cargas de trabajo de copia de seguridad y recuperación

Las cargas de trabajo de Backup and Recovery también se consideran recursos. Puedes asignar permisos a los miembros para que accedan a las cargas de trabajo de Backup and Recovery asociándolas a flotas. Por ejemplo, asigna a un miembro acceso a una carga de trabajo de Backup and Recovery asociándola a una flota a la que el miembro pueda acceder y otorgándole el rol adecuado de Backup and Recovery.

Consulta los recursos de tu organización

Consulta los recursos de tu organización para buscar un recurso específico y ver a qué flotas o carpetas está asociado. Si aún no has creado ninguna carpeta ni flota, todos los recursos están asociados a la flota

predeterminada directamente bajo la organización.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Recursos**.
3. Selecciona **Búsqueda avanzada y filtros**.
4. Utiliza las opciones disponibles para buscar un recurso:
   - **Buscar por nombre de recurso**: Introduce una cadena de texto y selecciona **Add**.
   - **Plataforma**: Selecciona una o varias plataformas, como Amazon Web Services.
   - **Recursos**: selecciona uno o varios recursos, como Cloud Volumes ONTAP.
   - **Organización, carpeta o flota**: selecciona toda la organización, una carpeta concreta o una flota concreta.
5. Selecciona **Buscar**.

Asocia un recurso con una carpeta o una flota

Asocia un recurso a una flota o carpeta para que los equipos correspondientes puedan gestionarlo. Por ejemplo, después de añadir un clúster ONTAP, asócialo a la flota `Production-US-East` para que los administradores regionales de almacenamiento de esa flota puedan gestionarlo.

Los usuarios con el rol de administrador de la organización pueden añadir recursos a una carpeta para delegar las tareas de asociación de flotas al administrador de la carpeta o al administrador de flotas de esa carpeta. "Asociar un recurso a una carpeta".

Pasos

1. Desde la página **Recursos**, navega hasta un recurso en la tabla, selecciona ••• y luego selecciona **Asociar a una carpeta o flota**.
2. Selecciona una carpeta o una flota y luego selecciona **Aceptar**.
3. Para asociar una carpeta o flota adicional, selecciona **Add folder or fleet** y luego selecciona la carpeta o la flota.

   Ten en cuenta que solo puedes seleccionar las carpetas y flotas para las que tienes permisos de administrador.

4. Selecciona **Asociar recursos**.
   - Si has asociado el recurso a flotas, los miembros que tengan permisos para esas flotas ahora pueden acceder al recurso desde la Console.
   - Si has asociado el recurso a una carpeta, un *administrador de carpetas o de flotas* ya puede acceder al recurso y asociarlo a una flota dentro de la carpeta. "Asociar un recurso a una carpeta".

Ver las carpetas y flotas asociadas a un recurso

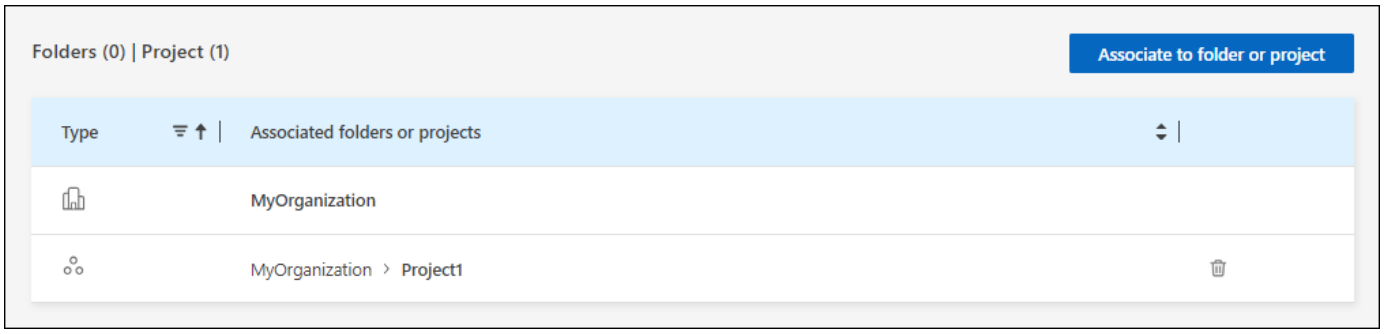
Comprueba a qué flotas o carpetas está asociado un recurso.

Para ver qué miembros tienen acceso al recurso, consulta los miembros asignados a la carpeta o flota correspondiente. "Gestiona las asignaciones de acceso a la flota".

Pasos

1. Desde la página **Recursos**, ve a un recurso de la tabla, selecciona ••• y luego selecciona **Ver detalles**.

El siguiente ejemplo muestra un recurso asociado a una flota.



Para ver qué miembros tienen acceso al recurso, consulta la carpeta o la flota correspondiente.

"Gestiona las asignaciones de acceso a la flota". "Gestiona el acceso de los miembros".

Eliminar un recurso de una carpeta o flota

Elimina la asociación de un recurso con una carpeta o una flota para evitar que los miembros lo gestionen ahí.

Para eliminar un sistema de almacenamiento de toda la organización, ve a la página **Sistemas** y elimina el sistema.

Pasos

1. Desde la página **Recursos**, ve a un recurso de la tabla, selecciona ••• y luego selecciona **Ver detalles**.
2. Para eliminar un recurso de una carpeta o flota, selecciona junto a la carpeta o flota.
3. Selecciona **Eliminar** para eliminar la asociación.

Mover un recurso entre flotas

Mueve un recurso de una flota a otra quitando su asociación con la flota actual y luego asociándolo con la flota de destino.

El acceso al recurso cambia en cuanto cambia la asociación. Si es posible, realiza ambos pasos en una sola ventana de mantenimiento.

Pasos

1. Desde la página **Recursos**, ve a un recurso de la tabla, selecciona ••• y luego selecciona **Ver detalles**.
2. Selecciona junto a la flota actual y selecciona **Eliminar**.
3. Selecciona **Add folder or fleet**.
4. Selecciona la flota de destino y selecciona **Aceptar**.
5. Selecciona **Asociar recursos**.

Información relacionada

- "Conoce la identidad y el acceso en NetApp Console"

- "Empieza con la identidad y el acceso en NetApp Console"
- "Gestiona las asignaciones de acceso a la flota después de mover recursos"
- "Conoce la API de identidad y acceso"

Agrega miembros a tu organización de implementación local de NetApp Console

Añade miembros a tu organización de implementación local de NetApp Console y asigna roles para conceder acceso a nivel de organización, carpeta o flota a usuarios, cuentas de servicio y usuarios del directorio.

Roles de acceso necesarios

Superadministrador, administrador de la organización o administrador de carpetas o flotas (para las carpetas y flotas que gestione). "Conoce los roles de acceso".

Antes de empezar

- Crea la jerarquía de carpetas y flotas que se adapte a tu organización. "Descubre cómo organizar tus recursos con carpetas y flotas".
- Asocia los recursos con las flotas correctas antes de asignar acceso a los miembros. "Aprende a gestionar los recursos en carpetas y flotas".
- Si vas a añadir un usuario del directorio, integra primero tu servicio de directorio. "Descubre cómo integrar con tu servicio de directorio".

Entiende cómo se concede el acceso en una implementación local de NetApp Console

La NetApp Console utiliza el control de acceso basado en roles (RBAC) para gestionar permisos. Asigna roles a los miembros para proporcionar el acceso necesario. Cada rol define las acciones permitidas para recursos específicos.

Ten en cuenta lo siguiente sobre la concesión de acceso en la implementación local de NetApp Console:

- Debes añadir explícitamente a cada usuario a tu organización y asignarle al menos un rol antes de que pueda acceder a recursos.
- Un rol que asignes a nivel de organización o de carpeta se hereda en los ámbitos subordinados, así que elige cuidadosamente el ámbito de asignación para darle acceso al miembro solo donde sea necesario. "Conoce la herencia de roles en la implementación local de NetApp Console".

Agrega miembros a tu organización

NetApp Console admite tres tipos de miembros: cuentas de usuario, usuarios de directorio y cuentas de servicio.

> Debes configurar primero un servidor de correo electrónico para usar con la implementación local de Console antes de poder añadir usuarios. "Aprende a configurar un servidor de correo electrónico."

Los usuarios del directorio se autentican a través de tu servicio de directorio integrado, pero aún así debes añadir a cada usuario del directorio de forma individual y asignar roles en la implementación local de Console. Crea cuentas de servicio directamente en Console.

Todos los miembros deben tener al menos un rol asignado explícitamente para poder acceder a la

implementación local de Console.

Al añadir a un miembro, selecciona la organización, la carpeta o la flota a la que deba tener acceso y asígnale el rol o los roles iniciales que necesite.

Agrega una cuenta de usuario

Debes tener el rol de Organization admin, Folder o fleet admin para añadir a un usuario a una organización, carpeta o flota, de modo que pueda acceder a los recursos.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Miembros**.
3. Selecciona **Add a member**.
4. Para **Tipo de miembro**, deja seleccionada la opción **Usuario**.
5. Para **Correo electrónico del usuario**, introduce la dirección de correo electrónico del usuario que está asociada con el inicio de sesión que creó.
6. Utiliza la sección **Seleccionar una organización, carpeta o flota** para elegir dónde necesita acceso el miembro.

   Ten en cuenta lo siguiente:

   - Solo puedes seleccionar las carpetas y flotas para las que tienes permisos.
   - Cuando seleccionas una organización o una carpeta, le das permisos al miembro sobre todo su contenido.
   - Solo puedes asignar el rol de **Organization admin** a nivel de organización.
7. **Selecciona una categoría** y luego selecciona un **rol** que le dé al miembro los permisos iniciales que necesita para la organización, la carpeta o la flota que seleccionaste.

   "Conoce los roles de acceso".

8. Para dar acceso a más carpetas, flotas o roles, selecciona **Add role**, elige la carpeta, la flota o la categoría de rol y selecciona un rol.
9. Selecciona **Add**.

   La consola envía las instrucciones por correo electrónico al usuario.

Agrega una cuenta de servicio

Añade una cuenta de servicio cuando necesites automatizar tareas o conectarte de forma segura a las API de Console. Después de crear la cuenta, copia su client ID y client secret para la integración que la vaya a usar.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Miembros**.
3. Selecciona **Add a member**.
4. En **Tipo de miembro**, selecciona **Service account**.
5. Introduce un nombre para la cuenta de servicio.

6. Utiliza la sección **Seleccionar una organización, carpeta o flota** para elegir dónde necesita acceso la cuenta de servicio.

   Ten en cuenta lo siguiente:

   - Solo puedes seleccionar las carpetas y flotas para las que tienes permisos.
   - Al seleccionar una organización o una carpeta, el miembro obtiene permisos sobre todo su contenido.
   - Solo puedes asignar el rol de **Organization admin** a nivel de organización.

7. Selecciona una **Categoría** y luego selecciona un **Rol** que le dé a la cuenta de servicio los permisos iniciales que necesita para la organización, la carpeta o la flota que seleccionaste.

   "Conoce los roles de acceso".

8. Para dar acceso a más carpetas, flotas o roles, selecciona **Add role**, elige la carpeta, la flota o la categoría de rol y selecciona un rol.
9. Descarga o copia el client ID y el client secret.

   La consola muestra el secreto de cliente solo una vez. Cópialo de forma segura; puedes volver a crearlo más adelante si lo pierdes.

10. Selecciona **Cerrar**.

Agrega un usuario de directorio a tu organización

Añade un usuario desde tu servicio de directorio integrado y asígnale sus primeros roles. Por ejemplo, añade un nuevo ingeniero de almacenamiento desde Active Directory y asígnale el rol de Storage admin en la flota `Production-US-East` para que pueda trabajar en esa flota.

Primero debes configurar tu servicio de directorio antes de poder añadir usuarios al directorio. "Descubre cómo integrar con tu servicio de directorio".

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Miembros**.
3. Selecciona **Add a member**.
4. En **Tipo de miembro**, selecciona **Directory user**.
5. En el campo **Correo electrónico del usuario**, introduce la dirección de correo electrónico del usuario del directorio que quieres añadir. Esta dirección de correo electrónico debe coincidir con la dirección de correo electrónico asociada al inicio de sesión del usuario en tu directorio.
6. Utiliza la sección **Seleccionar una organización, carpeta o flota** para elegir dónde necesita acceso el usuario del directorio.

   Ten en cuenta lo siguiente:

   - Solo puedes seleccionar las carpetas y flotas para las que tienes permisos.
   - Al seleccionar una organización o una carpeta, el miembro obtiene permisos sobre todo su contenido.
   - Solo puedes asignar el rol de **Organization admin** a nivel de organización.

7. Selecciona una **Categoría** y luego selecciona un **Rol** que le dé al usuario del directorio los permisos iniciales que necesita para la organización, la carpeta o la flota que seleccionaste.

"Conoce los roles de acceso".

8. Para conceder al usuario acceso adicional a otras carpetas, flotas o roles, selecciona **Add role**, elige la carpeta o flota, la categoría de rol y selecciona un rol.

Roles de acceso

NetApp roles de acceso para la implementación local de NetApp Console

La gestión de identidades y accesos (IAM) en la implementación local de NetApp Console ofrece roles predefinidos que puedes asignar a los miembros de tu organización en los distintos niveles de la jerarquía de recursos. Antes de asignar estos roles, debes entender los permisos que incluye cada rol. Los roles se clasifican en las siguientes categorías: plataforma, aplicación y servicio de datos.

Funciones de la plataforma

Los roles de la plataforma otorgan permisos de administración de la implementación local de NetApp Console, incluyendo la asignación de roles y la gestión de usuarios. La implementación local de NetApp Console cuenta con varios roles de la plataforma.

Función de la plataforma	Responsabilidades
"Administrador de la organización"	Permite a un usuario acceder sin restricciones a todas las flotas y carpetas dentro de una organización, añadir miembros a cualquier flota o carpeta, así como realizar cualquier tarea y usar cualquier servicio de datos que no tenga un rol explícito asociado. Los usuarios con este rol gestionan tu organización creando carpetas y flotas, asignando roles, añadiendo usuarios y gestionando sistemas si tienen las credenciales adecuadas.
"Administrador de carpetas o de flotas"	Permite a un usuario acceso sin restricciones a las flotas y carpetas asignadas. Puede añadir miembros a las carpetas o flotas que gestiona, además de realizar cualquier tarea y usar cualquier servicio de datos o aplicación en los recursos dentro de la carpeta o flota que tenga asignada.
"Administrador de la federación"	Permite a un usuario crear y gestionar federaciones de servicios de directorio con la Console para que los usuarios puedan autenticarse con sus credenciales de directorio existentes.
"Visor de la federación"	Permite a un usuario ver las federaciones de servicios de directorio existentes con la Console. No puede crear ni gestionar federaciones.
"Súper administrador"	Otorga al usuario todos los roles de administrador. Este rol está pensado para organizaciones más pequeñas que quizá no necesiten repartir las responsabilidades de la consola entre varios usuarios.
"Súper visualizador"	Otorga al usuario todos los roles de visualización. Este rol está pensado para organizaciones más pequeñas que quizá no necesiten distribuir las responsabilidades de la Console entre varios usuarios.

Funciones de la aplicación

A continuación se muestra una lista de roles de la categoría de aplicaciones. Cada rol otorga permisos

específicos dentro de su ámbito designado. Los usuarios que no tengan el rol de aplicación o de plataforma requerido no pueden acceder a la aplicación correspondiente.

Función de la aplicación	Responsabilidades
"Analista de soporte de operaciones"	Ofrece acceso a alertas y herramientas de supervisión, como la página Audit.
"Administrador de almacenamiento"	Administra las funciones de estado y gobernanza del almacenamiento, descubre recursos de almacenamiento, así como modifica y elimina sistemas existentes.
"Visor de almacenamiento"	Consulta el estado del almacenamiento y las funciones de gobernanza, así como los recursos de almacenamiento detectados anteriormente. No puedes detectar, modificar ni eliminar sistemas de almacenamiento existentes.
"Especialista en estado del sistema"	Administra las funciones de almacenamiento, estado y gobernanza, y tiene todos los permisos del administrador de almacenamiento, excepto que no puede modificar ni eliminar sistemas existentes.

Roles de servicios de datos

A continuación se muestra una lista de roles en la categoría de servicio de datos. Cada rol otorga permisos específicos dentro de su ámbito 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.

Función de servicio de datos	Responsabilidades
"Superadministrador de backup and recovery"	Realiza cualquier acción en NetApp Backup and Recovery.
"Administrador de copias de seguridad y recuperación"	Realiza copias de seguridad en instantáneas locales, replica en almacenamiento secundario y haz copias de seguridad en almacenamiento de objetos.
"Administrador de backup and recovery y restauración"	Restaura cargas de trabajo en Backup and Recovery.
"Administrador de backup, recovery y clonación"	Clona aplicaciones y datos en Backup and Recovery.
"Visor de copias de seguridad y recuperación"	Ver información sobre NetApp Backup and Recovery.
Visor de clasificación	Permite a los usuarios ver los resultados del escaneo 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 activar ni desactivar la exploración de volúmenes, buckets o esquemas de bases de datos. Data Classification no tiene un rol de administrador.

Función de servicio de datos	Responsabilidades
Administrador de SnapCenter	Ofrece la posibilidad de realizar copias de seguridad de instantáneas de clústeres ONTAP locales usando NetApp Backup and Recovery for applications. Un miembro que tenga este rol puede realizar las siguientes acciones: * Realizar cualquier acción desde Backup and Recovery > Applications * Gestionar todos los sistemas de las flotas y carpetas para las que tenga permisos * Utilizar todos los servicios de NetApp Console SnapCenter no tiene un rol de visualizador.

Enlaces relacionados

- "Conoce la gestión de identidades y accesos de NetApp Console"
- "Empieza con la identidad y el acceso en NetApp Console"
- "Agrega miembros y asigna roles en una organización de NetApp Console"
- "Conoce la API para NetApp Console IAM"

NetApp roles de acceso a la plataforma de implementación local de NetApp Console

Asigna roles de la plataforma a los usuarios para conceder permisos para gestionar la implementación local de la NetApp Console, asignar roles, añadir usuarios, crear flotas y gestionar la autenticación de usuarios.

Ejemplo de funciones organizativas para una gran empresa multinacional

XYZ Corporation organiza el acceso al almacenamiento de datos por regiones—América del Norte, Europa y Asia-Pacífico—, proporcionando control regional con supervisión centralizada.

El **administrador de la organización** en la implementación local de la Console de XYZ Corporation crea una organización inicial y carpetas independientes para cada región. El **administrador de carpetas o flotas** de cada región organiza las flotas (con los recursos asociados) dentro de la carpeta de la región.

Los administradores regionales con el rol de **Administrador de carpetas o flotas** gestionan activamente sus carpetas añadiendo recursos y usuarios. Estos administradores regionales también pueden añadir, eliminar o renombrar las carpetas y flotas que gestionan. El **Administrador de la organización** hereda los permisos para cualquier recurso nuevo, manteniendo la visibilidad del uso del almacenamiento en toda la organización.

Dentro de la misma organización, a un usuario se le asigna el rol de **Federation admin** para gestionar la federación de la organización con su IdP corporativo. Este usuario puede añadir o eliminar organizaciones federadas, pero no puede gestionar usuarios ni recursos dentro de la organización. El **Organization admin** asigna a un usuario el rol de **Federation viewer** para que compruebe el estado de la federación y vea las organizaciones federadas.

Las siguientes tablas indican las acciones que puede realizar cada rol de la plataforma de implementación local de Console.

Funciones de administración de la organización

Tarea	Administrador de la organización	Administrador de carpetas o de flotas
Crear, modificar o eliminar sistemas desde la implementación local de la NetApp Console (añadir o descubrir sistemas)	Sí	Sí
Crear carpetas y flotas, incluida la eliminación	Sí	No
Cambiar el nombre de las carpetas y flotas existentes	Sí	Sí
Asignar roles y añadir usuarios	Sí	Sí
Asocia recursos con carpetas y flotas	Sí	Sí
Regístrate para recibir asistencia y envía tus incidencias a través de la Console	Sí	Sí
Utiliza servicios de datos que no estén asociados a un rol de acceso explícito	Sí	Sí
Consulta la página de auditoría y las notificaciones	Sí	Sí

Funciones de la federación

Tarea	Administrador de la federación	Visor de la federación
Crear y actualizar integraciones de servicios de directorio	Sí	No
Ver federaciones y sus detalles	Sí	Sí

Roles de superadministrador y de visualizador

El rol de **Super admin** ofrece acceso completo para gestionar las funciones de Console, el almacenamiento y los servicios de datos. Este rol es adecuado para quienes supervisan la administración y la gobernanza. Por el contrario, el rol de **Super viewer** ofrece acceso de solo lectura, ideal para auditores o partes interesadas que necesitan visibilidad sin realizar cambios.

Las organizaciones deben utilizar el acceso de **Super admin** con moderación para minimizar los riesgos de seguridad y alinearse con el principio del privilegio mínimo. La mayoría de las organizaciones deberían asignar roles detallados con solo los permisos necesarios para reducir el riesgo y mejorar la auditabilidad.

Ejemplo de superroles

ABC Corporation cuenta con un pequeño equipo de cinco personas que utiliza la NetApp Console para servicios de datos y gestión del almacenamiento. En lugar de distribuir múltiples roles, asignan el rol de **Super admin** a dos miembros sénior del equipo, quienes se encargan de 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 **Super viewer**, lo que les permite supervisar la salud del almacenamiento y el estado de los servicios de datos sin poder modificar la configuración.

Función	Roles heredados
Súper administrador	• Administrador de la organización • Administrador de carpetas o de flotas • Superadministrador de backup and recovery • Administrador de almacenamiento
Súper visualizador	• Visor de organización • Visor de copias de seguridad • Visor de almacenamiento

Función de acceso de analista de soporte operativo en la implementación local de NetApp Console

En la implementación local de NetApp Console, puedes asignar el rol de analista de soporte operativo a los usuarios para darles acceso a las alertas y al monitoreo.

Analista de soporte operativo

Tarea	Puede realizar
Ver sistemas de almacenamiento	Sí
Consulta la página de auditoría y las notificaciones	Sí
Ver, descargar y configurar alertas	Sí

Roles de acceso al almacenamiento para la implementación local de NetApp Console

Puedes asignar los siguientes roles a los usuarios para darles acceso a las funciones de gestión del almacenamiento en la implementación local de NetApp Console. Puedes asignar a los usuarios un rol administrativo para gestionar el almacenamiento o un rol de visualización para monitorear.

Los administradores pueden asignar roles de almacenamiento a los usuarios para los siguientes recursos de almacenamiento y funciones:

Recursos de almacenamiento:

- Clústeres de ONTAP locales

Servicios y funciones de la consola:

- Funciones de estado del almacenamiento

Ejemplo de roles de almacenamiento en una implementación local de NetApp Console

XYZ Corporation, una empresa multinacional, cuenta con un amplio equipo de ingenieros y administradores de almacenamiento. Permiten a este equipo gestionar los activos de almacenamiento de sus regiones mientras limitan el acceso a tareas principales de implementación local de Console como la gestión de usuarios y la gestión de licencias.

Dentro de un equipo de 12 personas, a dos usuarios se les asigna el rol de **Storage viewer**, que les permite supervisar los recursos de almacenamiento asociados a las flotas de implementación local de Console a las que están asignados. A los nueve restantes se les asigna el rol de **Storage admin**, que incluye la capacidad de gestionar actualizaciones de software, acceder a ONTAP System Manager a través de la implementación local de Console, así como descubrir recursos de almacenamiento (añadir sistemas). A una persona del equipo se le asigna el rol de **System health specialist** para que pueda gestionar el estado de los recursos de almacenamiento de su región, pero sin poder modificar ni eliminar ningún sistema. Esta persona también puede realizar actualizaciones de software en los recursos de almacenamiento de las flotas a las que está asignada.

La organización cuenta con dos usuarios adicionales con el rol de **Organization admin** que pueden gestionar todos los aspectos de la implementación local de la Console, incluida la gestión de usuarios y de licencias, así como varios usuarios con el rol de **Folder or fleet admin** que pueden realizar tareas de administración de la implementación local de la Console para las carpetas y flotas a las que están asignados.

La siguiente tabla muestra las acciones que realiza cada rol de almacenamiento.

Función y acción	Administrador de almacenamiento	Especialista en estado del sistema	Visor de almacenamiento
Gestión del almacenamiento:			
Descubre nuevos recursos (agregar sistemas)	Sí	Sí	No
Ver sistemas añadidos	Sí	Sí	No
Eliminar sistemas desde la consola	Sí	No	No
Modificar sistemas	Sí	No	No
Acceso de system manager			
Puedes introducir tus credenciales	Sí	Sí	No

NetApp roles de Backup and Recovery en la implementación local de NetApp Console

En una implementación local de NetApp Console, puedes asignar los siguientes roles a los usuarios para darles acceso a NetApp Backup and Recovery dentro de la Console. Los roles de Backup and Recovery te dan la flexibilidad de asignar a los usuarios un rol específico para las tareas que necesitan realizar dentro de tu organización. Cómo asignes los roles depende de tu propio negocio y de tus prácticas de gestión del almacenamiento.

El servicio utiliza los siguientes roles que son específicos de NetApp Backup and Recovery.

- **Superadministrador de backup y recuperación**: Realiza cualquier acción en NetApp Backup and Recovery.

- **Administrador de backup and recovery**: Realiza copias de seguridad en instantáneas locales, replica en almacenamiento secundario y haz copias de seguridad en almacenamiento de objetos en NetApp Backup and Recovery.
- **Administrador de backup and recovery restore**: Restaura cargas de trabajo usando NetApp Backup and Recovery.
- **Administrador de clonación de backup y recuperación**: Clona aplicaciones y datos usando NetApp Backup and Recovery.
- **Visor de copias de seguridad y recuperación**: puedes ver la información en NetApp Backup and Recovery, pero no realizar ninguna acción.

Para obtener detalles sobre todos los roles de acceso de NetApp Console, consulta "la documentación sobre la configuración y la administración de la Console".

Roles utilizados para acciones habituales

La siguiente tabla indica las acciones que cada rol de NetApp Backup and Recovery puede realizar para todas las cargas de trabajo.

Función y acción	Superadministrador de backup and recovery	Administrador de copias de seguridad y recuperación	Administrador de backup and recovery y restauración	Administrador de backup, recovery y clonación	Visor de copias de seguridad y recuperación
Agregar, editar o eliminar hosts	Sí	No	No	No	No
Instalar complementos	Sí	No	No	No	No
Agrega credenciales (host, instancia, vCenter)	Sí	No	No	No	No
Ver el panel de control y todas las pestañas	Sí	Sí	Sí	Sí	Sí
Empieza tu prueba gratuita	Sí	No	No	No	No
Iniciar la detección de cargas de trabajo	No	Sí	Sí	Sí	No
Ver información sobre la licencia	Sí	Sí	Sí	Sí	Sí
Activar licencia	Sí	No	No	No	No
Ver hosts	Sí	Sí	Sí	Sí	Sí
Horarios:					
Activar programaciones	Sí	Sí	Sí	Sí	No

Función y acción	Superadministrador de backup and recovery	Administrador de copias de seguridad y recuperación	Administrador de backup and recovery y restauración	Administrador de backup, recovery y clonación	Visor de copias de seguridad y recuperación
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 política	Sí	Sí	No	No	No
Informes:					
Ver informes	Sí	Sí	Sí	Sí	Sí
Crear informes	Sí	Sí	Sí	Sí	No
Eliminar informes	Sí	No	No	No	No
Importar desde SnapCenter y gestionar el host:					
Ver los datos importados de SnapCenter	Sí	Sí	Sí	Sí	Sí
Importar datos desde SnapCenter	Sí	Sí	No	No	No
Gestionar (migrar) host	Sí	Sí	No	No	No
Configura los ajustes:					
Configura el directorio de registros	Sí	Sí	Sí	No	No
Asociar o eliminar credenciales de instancia	Sí	Sí	Sí	No	No
Buckets:					
Ver buckets	Sí	Sí	Sí	Sí	Sí

Función y acción	Superadministrador de backup and recovery	Administrador de copias de seguridad y recuperación	Administrador de backup and recovery y restauración	Administrador de backup, recovery y clonación	Visor de copias de seguridad y recuperación
Crear, editar o eliminar un bucket	Sí	Sí	No	No	No

Roles usados para acciones específicas de la carga de trabajo

La siguiente tabla muestra las acciones que cada función de NetApp Backup and Recovery puede realizar para cargas de trabajo específicas.

Cargas de trabajo Kubernetes

Esta tabla indica las acciones que cada función de NetApp Backup and Recovery puede realizar para acciones específicas de cargas de trabajo de Kubernetes.

Función y acción	Superadministrador de backup and recovery	Administrador de copias de seguridad y recuperación	Administrador de backup and recovery y restauración	Visor de copias de seguridad y recuperación
Ver clústeres, espacios de nombres, clases de almacenamiento y recursos de la API	Sí	Sí	Sí	Sí
Agrega nuevos clústeres de Kubernetes	Sí	Sí	No	No
Actualizar las configuraciones del clúster	Sí	No	No	No
Eliminar clústeres de la gestión	Sí	No	No	No
Ver aplicaciones	Sí	Sí	Sí	Sí
Crear y definir nuevas aplicaciones	Sí	Sí	No	No
Actualizar las configuraciones de las aplicaciones	Sí	Sí	No	No
Eliminar aplicaciones de la gestión	Sí	Sí	No	No
Ver los recursos protegidos y el estado de las copias de seguridad	Sí	Sí	Sí	Sí

Función y acción	Superadministrador de backup and recovery	Administrador de copias de seguridad y recuperación	Administrador de backup and recovery y restauración	Visor de copias de seguridad y recuperación
Crea copias de seguridad y protege las aplicaciones con políticas	Sí	Sí	No	No
Desproteger aplicaciones y eliminar copias de seguridad	Sí	Sí	No	No
Ver los puntos de recuperación y los resultados del visor de recursos	Sí	Sí	Sí	Sí
Restaurar aplicaciones a partir de puntos de recuperación	Sí	No	Sí	No
Ver políticas de backup de Kubernetes	Sí	Sí	Sí	Sí
Crear políticas de backup de Kubernetes	Sí	Sí	Sí	No
Actualizar las políticas de backup	Sí	Sí	Sí	No
Eliminar políticas de backup	Sí	Sí	Sí	No
Ver hooks de ejecución y fuentes de hooks	Sí	Sí	Sí	Sí
Crear ganchos de ejecución y fuentes de ganchos	Sí	Sí	Sí	No
Actualizar los hooks de ejecución y las fuentes de hooks	Sí	Sí	Sí	No
Eliminar los hooks de ejecución y las fuentes de hooks	Sí	Sí	Sí	No
Ver plantillas de hooks de ejecución	Sí	Sí	Sí	Sí
Crear plantillas de ganchos de ejecución	Sí	Sí	Sí	No
Actualizar las plantillas de los hooks de ejecución	Sí	Sí	Sí	No

Función y acción	Superadministrador de backup and recovery	Administrador de copias de seguridad y recuperación	Administrador de backup and recovery y restauración	Visor de copias de seguridad y recuperación
Eliminar plantillas de ganchos de ejecución	Sí	Sí	Sí	No
Ver el resumen de la carga de trabajo y los paneles de análisis	Sí	Sí	Sí	Sí
Ver buckets y destinos de almacenamiento de StorageGRID	Sí	Sí	Sí	Sí

Configura las integraciones y los servicios de NetApp Console

Integra la implementación local de NetApp Console con Active Directory

Integra la implementación local de NetApp Console con Active Directory para el inicio de sesión respaldado por directorio y la búsqueda de usuarios. Usa tu servicio de directorio para autenticar a los usuarios y luego asígnales acceso en la implementación local de NetApp Console.

Roles de acceso necesarios

Superadministrador o administrador de la organización. "Conoce los roles de acceso".

Cuando integras con Active Directory, la implementación local de Console autentica a los usuarios a través de tu directorio existente. Después de agregar un usuario del directorio, asígnale roles de acceso a Console para controlar a qué puede acceder ese usuario.

La integración con Active Directory también te ayuda a cumplir los requisitos de cumplimiento al aplicar tus controles, registros de auditoría y políticas existentes al acceso local de Console.

- La integración con Active Directory no crea grupos federados, no sincroniza las asignaciones de grupos del directorio y no concede acceso automáticamente. Los administradores siguen añadiendo usuarios del directorio a la organización y asignando roles en la implementación local de Console.
- Solo se admite una integración con Active Directory a la vez. Una vez configurada una integración, el botón **Add integration** queda desactivado. Para cambiar a otro directorio, primero debes desactivar o eliminar la integración existente.
- Los usuarios del directorio no configuran ni usan la autenticación multifactor (MFA). La implementación local de NetApp Console solo admite MFA para usuarios locales. "Aprende a gestionar la configuración de seguridad de los miembros".

Antes de empezar

Antes de integrar con Active Directory, comprueba que tienes:

- Un dominio de Active Directory y credenciales que permitan consultar el directorio
- La dirección del servidor LDAP y el nombre distintivo (DN) base del árbol de directorios
- Acceso de red desde la implementación local de Console a tu servidor LDAP en el puerto 389 (LDAP) o 636 (LDAPS)
- Certificados SSL/TLS, si tienes pensado utilizar LDAPS

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Directory services** para abrir la página Federations.
3. Selecciona **Add integration**.
4. Introduce los datos de conexión de tu servidor de Active Directory:
   - Un nombre descriptivo para la integración.
   - El **host LDAP**: nombre de host o dirección IP de tu servidor LDAP. Si hay varios servidores, introduce el principal.
   - El puerto: 389 para LDAP o 636 para LDAPS.
   - El **tiempo de espera de conexión** en milisegundos. El valor predeterminado es 1000 ms.
5. Selecciona **Usar SSL/TLS** para utilizar LDAPS. Asegúrate de que tu servidor LDAP sea compatible con LDAPS y que NetApp Console pueda acceder a los certificados necesarios.
6. Comprueba la conexión. Si falla, comprueba el host LDAP, el puerto, la conectividad de red y los certificados SSL/TLS.
7. Después de que la prueba finalice con éxito, introduce los datos del directorio y del usuario:
   - **Enlace al DN base**: Introduce el DN de enlace de la cuenta LDAP/AD que esta aplicación utilizará para conectarse al directorio, e introduce la credencial de enlace (contraseña) de dicha cuenta. NetApp Console utiliza estos datos para establecer el enlace con LDAP y validar la conexión.
   - **DN de usuario**: una cuenta de usuario con permiso para consultar el directorio. Por ejemplo, `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. Selecciona **Add** para guardar la integración.

Después de que termines

Después de guardar la integración, añade usuarios de directorio a tu organización y asígnales roles. Debes configurar y habilitar al menos una integración con Active Directory antes de poder añadir usuarios de directorio. "Aprende a añadir usuarios del directorio y a asignarles roles".

Desactivar o activar una integración con Active Directory

Desactiva una integración para suspender temporalmente la autenticación basada en un directorio sin eliminar la configuración. Cuando desactivas un servicio de directorio, los usuarios de ese directorio no pueden iniciar sesión a través del directorio.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Directory services** para abrir la página Federations.
3. En la lista de integraciones, busca la integración y selecciona el menú de acciones de esa fila.
4. Selecciona **Desactivar** para suspender la integración o **Activar** para restablecerla.

Eliminar una integración con Active Directory

Elimina una integración para borrar de forma permanente la configuración del servicio de directorio. Antes de eliminar, revisa cualquier advertencia sobre los usuarios del directorio que están vinculados a la integración, ya que su acceso se verá afectado.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Directory services** para abrir la página Federations.
3. En la lista de integraciones, busca la integración y selecciona el menú de acciones de esa fila.
4. Selecciona **Eliminar** y confirma la eliminación.

Conecta tu LLM y activa el asistente de NetApp Console en la implementación local de NetApp Console

Conecta tu modelo de lenguaje a gran escala (LLM) a NetApp Console en una implementación local para habilitar el asistente de la Console y la gestión del almacenamiento asistida por IA.

> Esta documentación sobre cómo conectar un modelo de lenguaje grande (LLM) al asistente de la Consola para habilitar funciones de IA se ofrece como una versión preliminar tecnológica. Con esta versión preliminar, NetApp se reserva el derecho a modificar los detalles de la oferta, los contenidos y el calendario antes de su disponibilidad general.

Roles de acceso necesarios

Superadministrador o administrador de la organización. "Conoce los roles de acceso".

Después de la configuración, los usuarios abren el asistente de la consola desde el panel de control y eligen un modo de acceso:

- En el modo **Solo lectura**, el asistente responde a las preguntas y ofrece orientación sin realizar cambios.
- En el modo **lectura/escritura**, el asistente puede realizar acciones en la infraestructura de almacenamiento. Muestra los detalles para revisión y confirmación antes de cada cambio. Para operaciones asíncronas, como la creación de volúmenes, crea una tarea que los usuarios pueden consultar desde el asistente.

Para conectar tu LLM, selecciona una ruta de proveedor, introduce los datos del endpoint y la clave de API, y luego selecciona un modelo en **Administración > Herramientas de IA**. Las acciones del asistente se mantienen dentro de tus políticas de almacenamiento y los controles de acceso basados en roles.

Reúne todo lo que necesites antes de conectar un LLM

Antes de conectar tu LLM, reúne lo siguiente:

- Tu elección del tipo de proveedor: OpenAI o OpenAI-compatible. "Infórmate sobre las opciones de proveedores."
- Una clave API válida para la ruta del proveedor que selecciones.
- La URL del endpoint para la ruta de tu proveedor.
- La URL de tu proxy o gateway, si tu organización lo requiere.

- Tu nombre de usuario o identificador de inicio de sesión único (SSO) para la cuenta del proveedor de LLM, si es necesario.
- Acceso a la red desde la implementación local de Console al endpoint seleccionado.
- Clases de almacenamiento y controles de acceso basados en roles para las acciones del asistente que planeas permitir.

Para obtener más información sobre los modelos compatibles, consulta "Infórmate sobre los proveedores y modelos de LLM compatibles en la implementación local de NetApp Console".

Conecta un LLM a la implementación local de NetApp Console

Introduce la configuración del proveedor, la clave API y el modelo para conectar tu LLM a la implementación local de Console.

Pasos

1. Inicia sesión en la consola local de NetApp Console.
2. Selecciona **Administración > Herramientas de IA**.
3. Selecciona el menú y, a continuación, selecciona **Editar**.
4. En **Tipo de proveedor**, selecciona un tipo de proveedor.

   "Infórmate sobre la integración de LLM en la implementación local de NetApp Console".

5. Si se te pide un endpoint del proveedor, introduce la URL del endpoint para la ruta del proveedor que seleccionaste.
6. Introduce la URL del proxy o de la puerta de enlace y las credenciales.
7. En el campo **Nombre de usuario**, introduce tu nombre de usuario o tu ID de SSO si la ruta de tu proveedor así lo requiere.
8. En el campo **Clave API**, pega la clave API de la ruta del proveedor que hayas seleccionado.
9. Selecciona un modelo de la lista.
10. Revisa la configuración y, a continuación, selecciona **Guardar**.

    Si falla el proceso de guardado o la prueba, verifica el tipo de proveedor, la URL del endpoint, la clave de API y el modelo seleccionado, y luego vuelve a intentarlo.

"Soluciona los problemas de tu integración con el LLM".

Comprueba que la integración de LLM funcione

Después de guardar la configuración, verifica la disponibilidad y el comportamiento del asistente.

Pasos

1. Comprueba que el botón **Asistente de la consola** aparece en el panel de control de implementación local de la NetApp Console.
2. Abre el asistente en modo **Solo lectura** y ejecuta una consulta básica.
3. Abre el asistente en modo **lectura/escritura** y confirma que las acciones que modifican el almacenamiento requieran la confirmación del usuario antes de ejecutarse.
4. Comprueba que los usuarios que necesitan flujos de trabajo de acciones dispongan de los controles de acceso basados en roles necesarios.

Una vez completada la validación, los usuarios pueden abrir el asistente de la Console desde el panel de control y describir las tareas en lenguaje sencillo. Para ver ejemplos de uso y flujos de trabajo de los usuarios finales, consulta "Usa el asistente de NetApp Console".

Protege las credenciales y supervisa el uso de los modelos de lenguaje grande (LLM)

- Siempre que sea posible, utiliza una clave API dedicada para la integración con la implementación local de Console.
- Rota las claves de la API según la política de tu organización.
- Restringe quién puede editar la configuración de las herramientas de IA solo a los roles de administrador necesarios.
- Supervisa el uso de la API por parte de los proveedores y las alertas para detectar actividad anómala o picos de costes.

Soluciona problemas de la integración de LLM en la implementación local de NetApp Console

Utiliza este flujo de clasificación rápida para diagnosticar y resolver problemas habituales de integración de LLM en NetApp Console en una implementación local.

> Esta documentación sobre cómo conectar un modelo de lenguaje grande (LLM) al asistente de la Consola para habilitar funciones de IA se ofrece como una versión preliminar tecnológica. Con esta versión preliminar, NetApp se reserva el derecho a modificar los detalles de la oferta, los contenidos y el calendario antes de su disponibilidad general.

Si aún no has completado la configuración, consulta "Conecta tu LLM y activa el asistente de NetApp Console".

Soluciona rápido los problemas de integración de Triage LLM

1. Valida la configuración de las herramientas de IA en **Administración > Herramientas de IA**.

   Confirma el tipo de proveedor, la URL del endpoint, la clave de API, el modelo seleccionado y el acceso a la red de salida.

2. Comprueba la disponibilidad del asistente en el panel de control.

   Comprueba que el botón **Console assistant** aparezca para los usuarios y las organizaciones previstos.

3. Valida el comportamiento en tiempo de ejecución.

   Realiza una solicitud sencilla de solo lectura y comprueba la accesibilidad del endpoint del proveedor, la disponibilidad del modelo y el estado del servicio del proveedor.

Solucionar problemas según los síntomas

Síntoma	Causa probable	Qué hay que comprobar	Próxima acción
Guardar o probar falla en AI Tools	Incompatibilidad de configuración o conectividad	Tipo de proveedor, URL del punto final, formato de la clave de API, modelo seleccionado y acceso saliente	Corrige el valor que no supera la validación y vuelve a guardar
Falta el botón **Console assistant**	Estado de integración inadecuado, incompatibilidad de la organización o incompatibilidad de RBAC	Guardado exitoso de herramientas de IA, estado de integración, organización actual y rol de acceso esperado	Actualiza la sesión y verifica con una cuenta de administrador que sepas que funciona correctamente
El asistente se abre pero la solicitud falla	Problema con el proveedor o con la ruta de ejecución	Accesibilidad del endpoint, disponibilidad del modelo en ese endpoint, límites del proveedor y estado temporal del proveedor	Vuelve a intentarlo tras solucionar la incompatibilidad entre el endpoint y el modelo o los problemas de límite por parte del proveedor.
La respuesta del asistente es lenta o irregular	Tamaño de la solicitud, rendimiento del endpoint o inestabilidad de la red/proxy	Prueba breve de respuesta, estado del servicio del proveedor y estabilidad de la red/proxy	Utiliza una instrucción más breve, prueba con otro modelo compatible y estabiliza la red o el enrutamiento del proxy

Responde ante la divulgación o el uso indebido de credenciales de LLM

Si sospechas que se ha filtrado una clave API o que se ha producido un uso no autorizado:

1. Revoca la clave API existente en el sistema de tu proveedor.
2. Crea una nueva clave de API.
3. Actualiza la clave en **Administración > Herramientas de IA**.
4. Verifica que la reconexión se realizó correctamente con una prueba de asistente de solo lectura.

Configura los canales de entrega de notificaciones en la implementación local de NetApp Console

En una implementación local de NetApp Console, puedes configurar varios canales para las notificaciones de alertas, incluyendo correo electrónico y webhooks.

Roles de acceso necesarios

Superadministrador o administrador de la organización. "Conoce los roles de acceso".

De forma predeterminada, la implementación local de Console muestra las notificaciones a través de su sistema de notificaciones integrado. Configurar canales de entrega adicionales te permite recibir notificaciones de la forma que mejor se adapte a tu flujo de trabajo.

Puedes enviar todas las notificaciones a través de los mismos canales o utilizar canales diferentes para distintos tipos de notificaciones. Por ejemplo, podrías enviar alertas urgentes sobre el almacenamiento por

correo electrónico, mientras que el resto de alertas se redirigen a una herramienta de monitorización de terceros mediante un webhook.

Una vez que hayas configurado los canales de envío de notificaciones, puedes configurar las reglas de notificación y asignarlas a los distintos canales. "Aprende a configurar las reglas de notificación".

Configura un servidor de correo electrónico

Cuando configuras un servidor de correo electrónico, la implementación local de Console envía notificaciones, alertas e invitaciones a usuarios a través de él. La implementación local de Console es compatible con servidores de correo electrónico SMTP, que pueden ser tu servidor de correo corporativo existente o un servicio de correo electrónico de terceros.

Pasos

1. Selecciona **Administración > Consola**.
2. Selecciona **Configuración** para abrir la página de configuraciones del sistema.
3. En la sección **Servidor de correo electrónico**, selecciona **Configurar**.
4. Introduce los datos de conexión de tu servidor de correo electrónico:
   - Agrega un nombre de remitente y una dirección de correo electrónico de remitente.
   - El **host SMTP**: nombre de host o dirección IP de tu servidor SMTP. Si tienes varios servidores, introduce el principal.
   - Selecciona el protocolo de conexión en la lista desplegable **Seguridad de la conexión**. El puerto ya está configurado y es de solo lectura: 25 para SMTP con STARTTLS o 465 para SMTPS.

     SMTPS (puerto 465) establece una conexión cifrada de forma inmediata y se recomienda para entornos donde la seguridad es importante. STARTTLS (puerto 25) actualiza desde una conexión no cifrada y puede volver a la transmisión no cifrada si falla la negociación del cifrado.
5. Selecciona **Test email** para enviar un correo de prueba al destinatario que indiques.
6. Después de que la prueba finalice con éxito, selecciona **Guardar** para guardar la configuración.

   Si la prueba falla, vuelve a verificar la configuración que introdujiste y asegúrate de que la implementación local de Console tenga acceso a la red del servidor de correo electrónico.

Actualizar la configuración de un servidor de correo electrónico

Puedes actualizar la configuración de un servidor de correo electrónico ya existente si quieres usar otro servidor de correo electrónico.

Pasos

1. Selecciona **Administración > Consola**.
2. Selecciona **Configuración** para abrir la página de configuraciones del sistema.
3. En la sección **Servidor de correo electrónico**, selecciona **Configurar**.
4. Selecciona **Borrar campos** para borrar la configuración actual.
5. Introduce los nuevos datos de conexión de tu servidor de correo electrónico.
6. Selecciona **Test email** para enviar un correo de prueba al destinatario que indiques.
7. Después de que la prueba se realice con éxito, selecciona **Guardar** para guardar la nueva configuración.

Si la prueba falla, vuelve a verificar la configuración que introdujiste y asegúrate de que la implementación local de Console tenga acceso a la red del servidor de correo electrónico.

Eliminar la configuración de un servidor de correo electrónico

Puedes eliminar la configuración del servidor de correo electrónico si ya no quieres que la implementación local de Console envíe correos electrónicos.

Pasos

1. Selecciona **Administración > Consola**.
2. Selecciona **Configuración** para abrir la página de configuración de sistemas.
3. En la sección **Servidor de correo electrónico**, selecciona **Configurar**.
4. Selecciona **Borrar campos** para borrar la configuración actual.
5. Selecciona **Guardar** para guardar la configuración borrada, lo que elimina la configuración del servidor de correo electrónico de la implementación local de Console.

Configura un webhook

Configura webhooks para enviar notificaciones desde la implementación local de Console a otras herramientas o servicios. Puedes configurar varios webhooks, cada uno apuntando a un endpoint diferente. Por ejemplo, uno para un SIEM y otro para un servicio de avisos de guardia.

Después de crear un webhook, los usuarios con el rol de Storage admin pueden asignarlo a reglas de alerta específicas. Por ejemplo, pueden enviar alertas críticas por correo electrónico mientras envían todas las alertas a una herramienta de monitorización de terceros a través de un webhook.

La implementación local de la consola no aplica control de acceso a los endpoints de webhook. Cualquier usuario o sistema que pueda acceder a la URL del endpoint recibe los datos de la alerta. Asegúrate de que el acceso a la aplicación receptora esté restringido a los usuarios autorizados mediante los propios controles de acceso de esa aplicación.

Antes de empezar

Confirma que la implementación local de Console pueda comunicarse con la aplicación receptora a través de la red y recopila la URL del endpoint, el método HTTP y cualquier detalle de autenticación o certificado que requiera esa aplicación.

Pasos

1. Selecciona **Administración > Consola**.
2. Selecciona **Configuración** para abrir la página de configuraciones del sistema.
3. En la sección **Integración de webhooks**, selecciona **Configurar**.
4. Introduce los datos necesarios para el webhook:
   - Un nombre descriptivo para el webhook.
   - La URL del punto final proporcionada por la aplicación receptora.
   - Método HTTP
   - Opcional: un certificado autofirmado en formato PEM.
   - Cualquier encabezado o secreto requerido (credenciales de autenticación).
   - El formato que se debe utilizar al enviar el webhook. Se admiten JSON y OTEL (OpenTelemetry).

Utiliza JSON para webhooks de uso general y puntos finales REST personalizados. Utiliza OTEL para plataformas de observabilidad que consumen de forma nativa señales de OpenTelemetry, como Grafana u otros colectores compatibles con OpenTelemetry.

5. Selecciona **Probar webhook** para comprobar la conexión del webhook y asegurarte de que la implementación local de Console puede enviar mensajes correctamente a la aplicación receptora.
6. Después de que la prueba se realice correctamente, selecciona **Guardar** para crear el webhook.

   Una vez que guardes el webhook, estará disponible para que los usuarios lo seleccionen donde se admitan webhooks, como en las opciones de entrega de alertas. "Descubre cómo crear reglas de alerta y asignar webhooks para el envío de alertas."