NetApp Console implementación local

NetApp Console local deployment

NetApp
August 10, 2026

Tabla de contenidos

NetApp Console implementación local

Notas de publicación

Novedades en la implementación local de NetApp Console

Descubre las nuevas funciones y mejoras en la última versión de la implementación local de la NetApp Console.

Presentación de la implementación local de NetApp Console

"Aprende a implementar localmente la NetApp Console".

Limitaciones conocidas en la implementación local 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. Revisa estas limitaciones cuidadosamente.

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

Limitaciones de la consola VM

Posible conflicto con direcciones IP en los rangos 10.42.0.0/16 y 10.43.0.0/16

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.

No se admiten servidores Linux compartidos

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

Agentes y extensiones de terceros

La máquina virtual del agente no admite agentes de terceros ni extensiones de máquina virtual.

Compara la implementación local de NetApp Console y NetApp Console

Elige NetApp Console si gestionas entornos en la nube y locales y quieres que NetApp se encargue de la infraestructura de la plataforma. Elige la implementación local de NetApp Console si gestionas un gran entorno ONTAP local y necesitas soberanía de datos total y gestión de almacenamiento condicionada por políticas.

NetApp Console

NetApp aloja y mantiene NetApp Console como una aplicación SaaS. Te registras y empiezas a gestionar el almacenamiento de inmediato. Para gestionar sistemas de almacenamiento, implementas agentes ligeros de Console en tus entornos en la nube o locales. Los agentes se conectan de forma saliente a la plataforma NetApp Console, y NetApp gestiona automáticamente la autenticación, las actualizaciones y la disponibilidad de la plataforma.

La NetApp Console también es compatible con el modo restringido (instalado en tu propia nube pública con conectividad saliente limitada) y el modo privado (instalado en tus propias instalaciones o en tu nube sin conectividad con la plataforma NetApp Console, incluidos los entornos air-gapped).

"Conoce los modos de implementación de NetApp Console".

NetApp Console es compatible con la gama más amplia de sistemas de almacenamiento, incluido el almacenamiento en la nube como Amazon FSx for ONTAP, Cloud Volumes ONTAP, Amazon S3, Google Cloud Storage, E-Series, StorageGRID y clústeres ONTAP locales. Ofrece acceso a la suite completa de servicios de datos de NetApp, incluyendo NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience, NetApp Copy and Sync y NetApp Data Classification. NetApp Console también ofrece funciones de contrato de soporte como Digital Advisor, Lifecycle Planning y paneles de sostenibilidad.

NetApp Console es ideal para organizaciones que gestionan entornos de nube híbrida y quieren la mayor cantidad de funciones, menos trabajo para mantener todo funcionando y licencias flexibles.

"Descubre NetApp Console^."

NetApp Console implementación local

La implementación local de NetApp Console te permite ejecutar el plano de control de NetApp Console íntegramente dentro de tu propia infraestructura local, sin que el tráfico de gestión salga de tu entorno. Despliegas la Console como una máquina virtual usando una imagen de dispositivo virtual y la gestionas como cualquier otra máquina virtual en tu entorno vCenter. No se requieren agentes de Console. La máquina virtual se comunica directamente con tus clústeres ONTAP.

Si bien el modo privado de NetApp Console también admite implementaciones aisladas físicamente y locales, la implementación local de Console está diseñada específicamente para la gestión de flotas ONTAP a escala empresarial. Aporta capacidades que no están disponibles en ningún modo de implementación de NetApp Console:

Políticas de clase de almacenamiento

Define las normas de almacenamiento una sola vez como plantillas reutilizables que agrupan los requisitos de rendimiento, capacidad y jerarquización. Todo el aprovisionamiento utiliza clases aprobadas, y la implementación local de Console supervisa continuamente las cargas de trabajo para verificar el cumplimiento e identifica las desviaciones.

Gestión de flotas

Organiza los clústeres en carpetas y flotas que reflejen la estructura de tu empresa, luego delega la administración a nivel de organización, carpeta o flota.

Analizador de carga de trabajo

Correlaciona la latencia, el rendimiento, las operaciones de entrada/salida por segundo y los cambios de configuración a lo largo del tiempo para detectar problemas de rendimiento antes de que afecten las cargas de trabajo.

Integración de modelos de lenguaje a gran escala

Conéctate a tu propio modelo de lenguaje a gran escala para aprovisionar almacenamiento usando lenguaje natural, investigar alertas y obtener respuestas contextuales sobre tu entorno de almacenamiento.

Corrección guiada y automatizada

Cuando una carga de trabajo se desvía de su clase de almacenamiento o se activa una alerta, la implementación local de Console ofrece recomendaciones de Fix-It. Usa los pasos guiados o la corrección automática con un solo clic para restablecer el cumplimiento sin pasos manuales.

Envío de alertas por correo electrónico y webhook

Configura los canales de notificación por correo electrónico y webhooks para que las alertas lleguen a los equipos adecuados cuando cambien las condiciones de almacenamiento. Los webhooks se integran con tus herramientas actuales de supervisión y gestión de incidencias.

El despliegue local de Console admite clústeres de ONTAP locales y NetApp Backup and Recovery. Se integra con Active Directory para la autenticación federada y admite la autenticación multifactor para usuarios locales.

La implementación local de la consola es la opción más adecuada para organizaciones con grandes entornos ONTAP locales que requieren un aprovisionamiento condicionado por políticas, comprobaciones de cumplimiento automatizadas y soberanía de datos total.

"Conoce la implementación local de NetApp Console^."

Comparativa de características

Gestión del almacenamiento

Característica	NetApp Console	NetApp Console implementación local
Clústeres de ONTAP locales	Sí (requiere Console agent)	Sí (comunicación directa desde la máquina virtual de la Console)
Sistemas de almacenamiento en la nube (Amazon FSx for ONTAP, Cloud Volumes ONTAP, Amazon S3 y otros)	Sí	No
E-Series y StorageGRID	Sí	No
NetApp Backup and Recovery	Sí	Sí
NetApp Disaster Recovery	Sí	No
NetApp Ransomware Resilience	Sí	No
NetApp Copy and Sync	Sí	No
NetApp Data Classification	Sí	No
Digital Advisor, Planificación del ciclo de vida, Sostenibilidad	Sí	No
Políticas de clases de almacenamiento y supervisión del cumplimiento	No	Sí
Corrección guiada y automatizada	No	Sí

Característica	NetApp Console	NetApp Console implementación local
Gestión de flotas (carpetas y flotas)	No	Sí
Analizador de carga de trabajo	No	Sí
Integración de modelos de lenguaje a gran escala para operaciones asistidas por IA	No	Sí

Configuración y seguridad de la consola

Característica	NetApp Console	NetApp Console implementación local
Modelo de implementación	Software como servicio, alojado por NetApp (hay diferentes modos de implementación disponibles)	Máquina virtual autohospedada en tu propia infraestructura
Agente de consola requerido	Sí	No
Actualizaciones de software	Automático, gestionado por NetApp	Manual
Acceso a la interfaz de usuario	NetApp Console aplicación (acceso a internet o a una máquina virtual)	Máquina virtual de consola (local, no requiere conexión a Internet)
Soberanía de datos	El tráfico de gestión va a la plataforma NetApp Console	No sale ningún dato ni tráfico de gestión de tu entorno
Integración con Active Directory	No	Sí
Federación de identidades	Sí	No
Autenticación multifactor (usuarios locales)	Sí	Sí
Registro de auditoría	Sí	Sí
Licencias	Suscripciones a Marketplace y trae tu propia licencia	Trae tu propia licencia

Empezar

Conoce la implementación local de NetApp Console

La implementación local de NetApp Console te permite alojar y ejecutar el plano de control autónomo de NetApp Console en tu propia infraestructura.

Disfrutarás de una gestión unificada del almacenamiento, la aplicación de políticas, la automatización a escala de parque informático y operaciones asistidas por IA. Ningún dato, metadato ni tráfico de gestión sale de tu entorno.

Implementa y opera Console en tu propia infraestructura

NetApp Console local deployment se ejecuta en tu propia infraestructura, así que tu equipo controla la

implementación, la conectividad y las operaciones diarias. Tú implementas el agente de Console, mantienes la máquina virtual de Console y gestionas las rutas de red necesarias para el tráfico de supervisión y gestión. Esto les da a los administradores empresariales control total sobre los límites operativos, mientras mantienen los datos de gestión dentro del entorno.

- "Instala el despliegue local de NetApp Console mediante una OVA en vCenter".
- "Realiza el mantenimiento de tu vCenter o host ESXi para la implementación local de NetApp Console".
- "Conoce los puertos para el agente de la Console local en la implementación local de NetApp Console".

Automatiza las operaciones de almacenamiento con API y cuentas de servicio

NetApp Console la implementación local admite integraciones basadas en API, así tu organización puede automatizar operaciones de almacenamiento repetitivas. Las cuentas de servicio permiten que las aplicaciones se autentiquen y operen con los roles asignados. El mismo control de acceso basado en roles y los controles de auditoría que se aplican a los usuarios interactivos rigen esas acciones. Esto permite la automatización empresarial mientras mantiene el acceso delimitado y responsable.

- "Agrega miembros a tu organización de implementación local de NetApp Console".
- "Conoce la API para NetApp Console IAM"

Controla el acceso mediante RBAC y la integración con Active Directory

NetApp Console local deployment proporciona control de acceso basado en roles (RBAC) de confianza cero que limita lo que los usuarios pueden ver y hacer dentro de las flotas y los recursos que gestionan. Puedes integrarlo con Active Directory para que los usuarios inicien sesión con sus credenciales corporativas existentes, y los usuarios locales pueden añadir autenticación multifactor (MFA) para otra capa de verificación. La gobernanza del acceso se mantiene alineada con las prácticas generales de gestión de identidades y accesos de tu organización.

- "Infórmate sobre la gestión de identidades y accesos en la implementación local de NetApp Console".
- "Infórmate sobre el acceso seguro a la implementación local de NetApp Console".

Organiza las flotas y delega la administración del almacenamiento

La implementación local de NetApp Console simplifica la administración mediante la organización de los recursos en carpetas y flotas. Puedes asignar flotas a entornos, unidades de negocio o regiones, y luego delegar la administración a nivel de organización, carpeta o flota para mantener clara la responsabilidad. Esta estructura ayuda a los equipos de almacenamiento grandes a distribuir el trabajo sin perder la coherencia de las políticas ni la gobernanza.

- "Conoce las carpetas y las flotas en la implementación local de NetApp Console".
- "Conoce las flotas de almacenamiento en la implementación local de NetApp Console".

Realiza un seguimiento y exporta la actividad administrativa para cumplir con la normativa

Cada acción administrativa genera un registro de auditoría. Los equipos de seguridad y cumplimiento pueden usar estos registros para investigar incidentes, mostrar la efectividad del control y cumplir con los requisitos de auditoría. Exporta los registros de auditoría a tu servidor syslog a través de un webhook para la supervisión centralizada, una retención más prolongada y análisis. Como el despliegue local de NetApp Console se ejecuta en tu propio entorno, los datos de los registros nunca salen de tu infraestructura.

- "Audita la actividad de implementación local de NetApp Console".

Provisiona almacenamiento de forma coherente con las políticas de clase de almacenamiento

NetApp Console local deployment garantiza un comportamiento coherente del almacenamiento mediante clases de almacenamiento, que son plantillas que agrupan políticas de rendimiento, capacidad y jerarquización en definiciones reutilizables. Los administradores definen los estándares de almacenamiento una sola vez. Los administradores y los flujos de trabajo automatizados usan esas clases aprobadas para toda la actividad de aprovisionamiento en tu entorno. Esto evita desviaciones en la configuración, reduce el tiempo que los administradores junior dedican a las decisiones de aprovisionamiento y garantiza que cada carga de trabajo cumpla de inmediato con los estándares de tu organización. Después del aprovisionamiento, Console local deployment sigue supervisando cada carga de trabajo para verificar el cumplimiento.

- "Descubre cómo gestionar el almacenamiento con la implementación local de NetApp Console".

Supervisa el cumplimiento de las clases de almacenamiento y corrige automáticamente cualquier desviación

La implementación local de NetApp Console supervisa cada carga de trabajo en función de la clase de almacenamiento utilizada para aprovisionarla. Cuando una carga de trabajo se desvía, ya sea por un cambio directo en la configuración del clúster o por un deterioro del rendimiento, la implementación local de NetApp Console señala la infracción de inmediato. Los administradores pueden seguir pasos de corrección guiados o configurar la corrección automatizada para resolver condiciones comunes de desviación sin intervención manual. Esta aplicación continua reduce el riesgo de auditoría y mantiene tu entorno en conformidad entre las revisiones programadas.

Supervisa la salud del almacenamiento y recibe alertas en todas las flotas

NetApp Console la implementación local te ofrece un único lugar desde el que supervisar el estado y el rendimiento de todos los clústeres que gestionas. Los paneles de control de toda la flota muestran los clústeres y volúmenes que necesitan atención. Los paneles personalizados permiten a los administradores crear vistas de supervisión que se adapten a sus responsabilidades. El Workload Analyzer correlaciona la latencia, el rendimiento, la utilización de recursos y los cambios de configuración a lo largo del tiempo para ayudarte a identificar las causas raíz antes de que los problemas afecten a las cargas de trabajo.

Configura los canales de envío por correo electrónico y webhook para que las alertas lleguen a los equipos adecuados cuando cambien las condiciones. Los administradores de la organización configuran los destinos, y los administradores de almacenamiento los aplican en las reglas de alerta para que las rutas de respuesta se ajusten a tu modelo operativo. Esto ayuda a los equipos de la empresa a responder más rápidamente ante incidentes relacionados con la capacidad, el rendimiento y la protección.

- "Infórmate sobre cómo supervisar el estado del almacenamiento en una implementación local de NetApp Console".
- "Configura los canales de entrega de notificaciones en la implementación local de NetApp Console".
- "Configura reglas de notificación para alertas en la implementación local de NetApp Console".

Provisiona almacenamiento e investiga alertas con lenguaje natural

NetApp Console la implementación local puede conectarse a tu propio modelo de lenguaje a gran escala (LLM) para ofrecer gestión del almacenamiento asistida por IA. Puedes describir una carga de trabajo en lenguaje sencillo para obtener un plan de aprovisionamiento, pedir a la Console que investigue una alerta activa u obtener respuestas contextuales sobre tu entorno de almacenamiento. Cada acción de IA se mantiene dentro de los límites de tus clases de almacenamiento y de los controles de acceso basados en roles que se aplican a tu cuenta, y debes confirmar las operaciones sensibles antes de que continúen. Console la implementación local envía solicitudes únicamente al endpoint del LLM que configuren tus administradores.

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

Haz copias de seguridad y restaura el almacenamiento con NetApp Backup and Recovery

Más allá de la configuración y la supervisión, la implementación local de NetApp Console te da acceso a NetApp Backup and Recovery para que puedas proteger tus datos desde la misma interfaz. Puedes hacer copias de seguridad y restaurar tus datos para cumplir con tus requisitos de protección y recuperación. Gestionar la protección de datos junto con tu almacenamiento mantiene la gobernanza coherente y reduce la cantidad de herramientas que tus equipos necesitan para operar.

- "Conoce los servicios de datos en la implementación local de NetApp Console".

Conoce la gestión de identidades y control de acceso en la implementación local de NetApp Console

La gestión de identidades y acceso (IAM) en la implementación local de NetApp Console controla quién puede iniciar sesión, cómo se verifican las identidades, a qué recursos pueden acceder los usuarios y qué acciones pueden realizar. En la implementación local de NetApp Console, IAM incluye el control de acceso basado en roles (RBAC), la autenticación multifactor (MFA) y la autenticación respaldada por directorios, así como la jerarquía y el modelo de auditoría que respaldan la administración delegada.

Utiliza esta página para comprender a grandes rasgos el modelo IAM de implementación local de la NetApp Console. Para ver ejemplos detallados de planificación de jerarquías, consulta "Conoce las carpetas y las flotas en la implementación local de NetApp Console".

> Debes tener los roles de *Super admin*, *Organization admin* o *Folder or fleet admin* para gestionar IAM en NetApp Console.

Qué significa IAM en la implementación local de NetApp Console

NetApp Console la implementación local de IAM combina la verificación de identidad, el control de acceso, la delegación y la auditabilidad:

- *La autenticación* determina cómo los usuarios inician sesión, ya sea con credenciales locales o a través de la configuración de tu directorio.
- *La autorización* determina qué pueden hacer los miembros después de iniciar sesión, según los roles predefinidos y el ámbito donde los asignes.
- *La jerarquía y el ámbito de aplicación* determinan a qué carpetas, flotas y recursos puede acceder un miembro.
- *La gestión de usuarios y credenciales* determina cómo añades usuarios, cuentas de servicio y cómo gestionas la MFA y los secretos de las cuentas de servicio.
- *Seguimiento de auditoría y cumplimiento* registra la actividad relacionada con IAM para que puedas revisar quién cambió el acceso y cuándo.

Cómo funciona la autenticación

NetApp Console la implementación local admite tanto identidades locales como la integración de identidades externas.

Puedes integrar la implementación local de NetApp Console con Active Directory para que los usuarios inicien sesión con sus credenciales corporativas existentes. Esto elimina la necesidad de contraseñas separadas en la implementación local de Console y permite a los administradores buscar usuarios del directorio al asignar acceso.

Para los usuarios locales, la autenticación multifactor (MFA) añade un paso de verificación adicional para reducir el riesgo de acceso no autorizado si las credenciales se ven comprometidas.

Para obtener más información sobre la autenticación y las opciones de inicio de sesión seguro, "Conoce el acceso seguro en la implementación local de NetApp Console".

Cómo funciona la autorización

Después de que un usuario inicia sesión, la implementación local de NetApp Console utiliza RBAC para determinar qué puede ver y hacer ese usuario.

La integración con Active Directory o LDAP se encarga de la autenticación. NetApp Console la autorización para la implementación local sigue siendo independiente: los administradores asignan roles predefinidos a nivel de organización, carpeta o flota para controlar a qué puede acceder cada miembro.

Un mismo rol otorga distintos niveles de acceso efectivo en función del ámbito en el que lo asignes. Este modelo te permite dar un acceso amplio a los administradores centrales, mientras que limita a los administradores regionales o de equipo a las flotas que gestionan.

Los roles que asignas a nivel de organización o de carpeta se heredan en los ámbitos subordinados. Este modelo de herencia es una parte clave de cómo NetApp Console delega el acceso entre carpetas y flotas.

NetApp diseña las funciones de implementación local de NetApp Console siguiendo los principios de privilegios mínimos, así que cada función incluye solo los permisos necesarios para sus tareas.

"Conoce el control de acceso basado en roles y la herencia de roles en la implementación local de NetApp Console".

Cómo funciona la jerarquía de IAM

La implementación local de NetApp Console utiliza una jerarquía para agrupar recursos y delimitar el acceso. La organización se encuentra en la parte superior, luego las carpetas, después las flotas y, finalmente, los recursos (incluidas las posibles subcarpetas) asociados a esas flotas.

Esta jerarquía es lo que hace posible la delegación. Por ejemplo, un administrador de la organización puede gestionar el acceso en toda la organización, mientras que un administrador de carpeta o de flota solo puede gestionar los recursos y los miembros dentro de la parte de la jerarquía que posee.

NetApp Console IAM se basa en tres tipos de componentes: componentes organizativos que definen la jerarquía, recursos que se asignan dentro de esa jerarquía y miembros y roles que controlan quién puede acceder a qué.

Dado que los roles se heredan a través de esta jerarquía, el diseño de tus carpetas y flotas influye directamente en el alcance de cada asignación de acceso.

"Descubre cómo añadir flotas a tu organización.".

Seguridad y credenciales de los miembros

IAM en la implementación local de NetApp Console también incluye controles operativos para proteger el

acceso de los miembros después de que existan las cuentas.

En el caso de los usuarios locales, los administradores pueden ayudar a los usuarios a recuperar el acceso indicando cómo restablecer la contraseña, eliminando o desactivando temporalmente la autenticación multifactor (MFA) y revisando el comportamiento de la MFA de los usuarios locales. En el caso de las cuentas de servicio, los administradores pueden volver a crear las credenciales cuando se pierden o se rotan los secretos.

Estos controles forman parte de la gestión de identidades y acceso (IAM), ya que determinan cómo se mantiene la seguridad de las identidades a lo largo del tiempo, no solo cómo se asigna el acceso inicialmente.

"Aprende a gestionar la seguridad de los miembros".

Auditar la actividad de IAM

IAM en la implementación local de NetApp Console incluye la posibilidad de revisar y exportar la actividad relacionada con el acceso.

Desde la página de Auditoría, puedes revisar las acciones relacionadas con la gestión de tu organización, como añadir miembros, crear flotas y asociar recursos. También puedes filtrar los registros de auditoría por el servicio Tenancy para centrarte en los cambios relacionados con IAM, o exportar los registros de auditoría a un sistema externo.

La auditabilidad es un principio importante de IAM porque te permite verificar quién cambió el acceso, cuándo ocurrió el cambio y si el cambio fue exitoso.

"Descubre cómo auditar la actividad de implementación local de NetApp Console".

Próximos pasos con IAM en NetApp Console

- "Empieza con la identidad y el acceso en NetApp Console"
- "Conoce el acceso seguro en la implementación local de NetApp Console"
- "Conoce RBAC en la implementación local de NetApp Console"
- "Supervisar o auditar la actividad de implementación local de Console"
- "Conoce la API para NetApp Console IAM"

Conoce la gestión de flotas en la implementación local de NetApp Console

La gestión de flotas en la implementación local de NetApp Console es la práctica de organizar los sistemas de almacenamiento en grupos lógicos para que puedas aplicar políticas coherentes, controlar el acceso y supervisar el estado de los clústeres relacionados. En lugar de gestionar cada clúster de forma independiente, la gestión de flotas te permite tratar tu flota como un conjunto común de recursos para cumplir tus objetivos de almacenamiento de datos.

A medida que tu entorno de almacenamiento crece, gestionar clústeres individuales deja de ser práctico. La gestión de flotas resuelve esto dándote una forma estructurada de agrupar sistemas relacionados, delegar responsabilidades y asegurarte de que cada clúster opere bajo los mismos estándares.

Por qué es importante la gestión de flotas

La gestión de flotas aborda tres retos fundamentales:

- **Simplificación mediante la abstracción** - la gestión de flotas elimina la complejidad que supone gestionar cada infraestructura de almacenamiento por separado. En lugar de tener que ocuparte de la configuración en clúster, gestionas tu parque de almacenamiento como un todo unificado, lo que reduce la carga operativa y la fatiga decisoria.
- **Coherencia y escalabilidad** - sin una organización clara, los distintos equipos toman decisiones diferentes para cargas de trabajo similares, lo que da lugar a configuraciones fragmentadas. La gestión de flotas te permite aplicar estándares en docenas de sistemas a la vez, lo que garantiza que las nuevas cargas de trabajo partan de la misma base de referencia en todos los equipos y flotas.
- **Gobernanza y control** - a medida que los equipos crecen, necesitas límites claros sobre quién puede gestionar qué. La gestión de flotas proporciona esos límites mediante una estructura organizativa y control de acceso, asegurando que las decisiones de almacenamiento sigan estando gobernadas y sean auditables.

Cómo las flotas organizan tus recursos

La jerarquía de recursos de tu organización está formada por carpetas y flotas:

Para obtener una descripción detallada de la jerarquía y el modelo de acceso, consulta "Conoce las carpetas y las flotas en la implementación local de NetApp Console".

- **Organización** - el nivel superior que representa a tu empresa.
- **Carpetas** - te ayudan a organizar flotas relacionadas. Por ejemplo, puedes crear una carpeta para cada región o unidad de negocio, y luego crear flotas dentro de cada carpeta. Las carpetas pueden contener otras carpetas o flotas. Cuando asignas un rol a nivel de carpeta, los miembros heredan ese rol para todas las flotas dentro de la carpeta.
- **Flotas** - agrupa los sistemas de almacenamiento que gestionas. Asocias los sistemas de almacenamiento a las flotas y asignas miembros a las flotas para darles acceso.

> Las carpetas son una herramienta de organización y no son visibles para los miembros que no tengan permisos de IAM, como los roles de Organization admin, Folder admin o Fleet admin. Los miembros acceden a las flotas, no a las carpetas.

Modelos habituales de organización de flotas

La forma de organizar las flotas depende de tu modelo operativo:

- **Por entorno** - crea flotas independientes para las cargas de trabajo de producción, desarrollo y prueba. Esto mantiene el almacenamiento de producción bajo políticas más estrictas, mientras permite más flexibilidad en los entornos de menor nivel.
- **Por unidad de negocio** - agrupa los clústeres que dan servicio a un departamento específico, como finanzas, ingeniería o recursos humanos, en una flota dedicada. Luego puedes asignar responsabilidades de gestión del almacenamiento a los miembros del equipo de esa unidad de negocio sin exponerles a otras flotas.
- **Por ubicación o centro de datos** - cuando los clústeres están distribuidos entre distintos emplazamientos, organizarlos por ubicación te permite supervisar el estado a nivel de emplazamiento, aplicar políticas específicas para cada región y realizar un seguimiento del consumo de capacidad por emplazamiento.

- **Por nivel de aplicación** - agrupa los clústeres que alojan un tipo específico de carga de trabajo, como bases de datos, recursos compartidos de archivos o máquinas virtuales, para que puedas aplicar normas coherentes y adaptadas a ese tipo de carga de trabajo en toda la flota.

Utiliza carpetas para añadir otro nivel de organización. Por ejemplo, crea una carpeta para cada región y luego crea flotas por entorno dentro de cada carpeta regional.

Cómo la gestión de flotas facilita el control de acceso

Las flotas y las carpetas sirven para delimitar el acceso de los usuarios y las responsabilidades administrativas:

- **Acceso a nivel de carpeta** - cuando asignas un rol a nivel de carpeta, el miembro hereda ese rol para todas las flotas y recursos dentro de la carpeta. Esto te permite delegar responsabilidades administrativas sin conceder acceso a toda la organización.
- **Acceso a nivel de flota** - cuando asignas un rol a nivel de flota, el miembro solo tiene acceso a los sistemas de almacenamiento dentro de esa flota. Esto te permite delegar la gestión del almacenamiento a miembros del equipo o a responsables de aplicaciones sin exponer partes no relacionadas de tu infraestructura.

La implementación local de la consola permite la supervisión del estado y el rendimiento a nivel de flota, así puedes ver el estado de todos los clústeres de una flota desde una sola vista, identificar problemas temprano y actuar antes de que afecten a las cargas de trabajo.

Cómo funciona la gestión del almacenamiento

La gestión del almacenamiento consiste en definir normas de almacenamiento, aplicarlas de forma coherente y gestionar las cargas de trabajo para que se mantengan alineadas a lo largo del tiempo. En la implementación local de Console, dichas normas se expresan como políticas de clase de almacenamiento y clases de almacenamiento, se aplican a flotas y se hacen cumplir mediante flujos de trabajo de aprovisionamiento regidos por RBAC y el registro de auditoría.

La implementación local de NetApp Console integra cuatro conceptos en un único flujo de trabajo:

- Las **flotas** definen el ámbito en el que gestionas el almacenamiento. Una flota agrupa sistemas para que puedas controlar el acceso, aplicar normas de forma coherente y gestionar los recursos como una unidad.
- Las **políticas de clase de almacenamiento** definen los estándares como módulos reutilizables (rendimiento, capacidad, seguridad, protección de datos).
- **Las clases de almacenamiento** expresan la finalidad de la carga de trabajo. Una clase de almacenamiento es una plantilla con nombre compuesta por una o más políticas.
- **Los flujos de trabajo de aprovisionamiento** crean almacenamiento dentro de unos límites preestablecidos. Los distintos flujos de trabajo toman decisiones de configuración de forma diferente, pero todos pueden aplicar clases de almacenamiento y siguen estando gobernados por RBAC y el registro de auditoría.

Enfoques de aprovisionamiento

La implementación local de NetApp Console admite tres métodos de aprovisionamiento, todos ellos regulados por RBAC, el registro de auditoría y las normas de clase de almacenamiento:

- **Aprovisionamiento manual** - Tú seleccionas el sistema de destino y especificas directamente los detalles de configuración. Usa esto cuando necesites un control explícito sobre la selección y la configuración del

sistema.

- **Aprovisionamiento automatizado** - tú proporcionas los datos de la carga de trabajo y, si lo deseas, seleccionas una clase de almacenamiento. La implementación local de NetApp Console recomienda la ubicación más adecuada y aplica ajustes basados en las clases para reducir las decisiones manuales.
- **Aprovisionamiento asistido por IA (agente)**: describes lo que necesitas en lenguaje natural. La implementación local de NetApp Console propone un plan sujeto a las restricciones de RBAC y clases de almacenamiento, y solo realiza el aprovisionamiento después de que lo revises y apruebes.

A dónde ir ahora

- Para conocer las normas de almacenamiento, consulta "Obtén información sobre las clases de almacenamiento y las políticas en el despliegue local de NetApp Console".
- Para crear y gestionar flotas, consulta "Gestiona carpetas y flotas".
- "Provisiona almacenamiento manualmente"
- "Provisiona almacenamiento automáticamente"
- "Provisiona almacenamiento con asistencia de IA"

Obtén información sobre las clases de almacenamiento y las políticas en el despliegue local de NetApp Console

Una clase de almacenamiento es una plantilla reutilizable que define cómo debe comportarse el almacenamiento. Cuando aprovisionas almacenamiento utilizando una clase de almacenamiento, NetApp Console local deployment aplica automáticamente los estándares codificados en esa clase sin que los administradores tengan que tomar decisiones de configuración individuales para cada carga de trabajo.

Las clases de almacenamiento se crean a partir de políticas de clases de almacenamiento, que definen aspectos concretos del comportamiento del almacenamiento. En conjunto, te permiten definir los estándares de almacenamiento de tu organización una sola vez y aplicarlos de forma coherente en todas las flotas.

Qué son las políticas de clase de almacenamiento

Una política de clase de almacenamiento define una dimensión del comportamiento del almacenamiento. Las políticas son elementos básicos reutilizables que combinas para crear clases de almacenamiento.

Entre los tipos de políticas más comunes se incluyen:

- **Políticas de rendimiento** - define los objetivos de latencia, las IOPS o los requisitos de rendimiento.
- **Políticas de capacidad** - define el modo de aprovisionamiento, las alertas de umbrales o los límites de crecimiento.
- **Políticas de seguridad** - define requisitos de cifrado, cumplimiento o control de acceso.
- **Políticas de protección de datos** - define las programaciones de snapshots, los destinos de replicación o los períodos de retención.

Defines las políticas de forma independiente y luego las combinas cuando creas una clase de almacenamiento. Esto te permite reutilizar la misma política de rendimiento en varias clases, o actualizar una política de capacidad en un solo lugar y aplicar ese cambio a todas las clases que la usan.

Qué son las clases de almacenamiento

Una clase de almacenamiento es una plantilla con nombre que se compone de una o varias políticas. Refleja los estándares de almacenamiento de tu organización para un tipo específico de carga de trabajo.

Por ejemplo, podrías crear una clase de almacenamiento **Production Database** que combine alto rendimiento, alta disponibilidad y políticas estrictas de protección de datos, o una clase de almacenamiento **Development File Share** que combine rendimiento moderado, capacidad flexible y políticas básicas de protección de datos.

Los administradores de almacenamiento definen clases de almacenamiento para plasmar los requisitos de la empresa. Toda la actividad de aprovisionamiento, ya sea manual, a través de flujos de trabajo guiados o mediante automatización, se basa en la biblioteca de clases que han aprobado esos administradores.

Cómo las clases de almacenamiento garantizan el cumplimiento de las normas

Cuando aprovisionas almacenamiento, seleccionas una clase de almacenamiento en lugar de configurar parámetros individuales. La implementación local de NetApp Console utiliza las políticas de esa clase para identificar qué clústeres de tu flota tienen la capacidad y el margen de rendimiento necesarios para soportar la carga de trabajo, recomendar la mejor opción de ubicación y aplicar automáticamente los ajustes definidos por la clase en el momento del aprovisionamiento.

Tras el aprovisionamiento, la implementación local de Console evalúa continuamente cada carga de trabajo en función de los estándares de su clase de almacenamiento.

Desviación de la clase de almacenamiento y cumplimiento

Cuando una carga de trabajo deja de ajustarse a la finalidad de su clase de almacenamiento, la implementación local de Console la marca para su investigación y corrección.

Los problemas se dividen en dos categorías:

- **Desviación de la configuración**: Los parámetros de almacenamiento regulados por la política de clase de almacenamiento ya no se corresponden con la configuración prevista. Esto puede ocurrir cuando se realizan cambios directamente en el clúster ONTAP o fuera de los flujos de trabajo estándar de aprovisionamiento de almacenamiento.
- **Incumplimiento de los requisitos de rendimiento**: El comportamiento en tiempo de ejecución de la carga de trabajo ya no cumple con la intención de rendimiento de la clase de almacenamiento (por ejemplo, una presión sostenida cerca de un límite de QoS o una latencia de cola elevada).

Una vista de análisis explica qué ha cambiado y por qué. Es posible que haya disponibles acciones de corrección guiadas (por ejemplo, **Fix it**) para ayudar a restablecer el cumplimiento. Algunas correcciones se pueden aplicar directamente, mientras que otras pueden requerir alinear la carga de trabajo a una clase de almacenamiento diferente para restablecer el comportamiento previsto.

Dónde investigar

Normalmente, puedes investigar las desviaciones y los incumplimientos desde una de estas ubicaciones (la disponibilidad depende de tu implementación y permisos):

- **Clases de almacenamiento:** Drift / Compliance
- **Alertas:** Analiza

Para obtener instrucciones paso a paso, consulta Corrige la desviación de la clase de almacenamiento.

Flujo de trabajo de principio a fin

Los pasos siguientes describen el proceso para utilizar las clases de almacenamiento con el fin de estandarizar y gestionar el almacenamiento en tu entorno:

1. **Crear políticas de clases de almacenamiento** - las políticas definen los distintos aspectos del comportamiento del almacenamiento (objetivos de rendimiento, ajustes de capacidad, requisitos de seguridad, calendarios de protección de datos). Crea las políticas antes de crear una clase de almacenamiento.
2. **Crear una clase de almacenamiento** - configura una clase de almacenamiento combinando una política de cada categoría aplicable. Puedes utilizar una clase de almacenamiento predefinida o crear una personalizada que se ajuste a las normas de tu organización.
3. **Asocia la clase de almacenamiento con una flota** - después de crear una clase de almacenamiento, asóciala a la flota donde se usará para el aprovisionamiento de almacenamiento y la supervisión del cumplimiento.
4. **Aprovisiona almacenamiento usando la clase de almacenamiento** - Cuando aprovisiones un volumen o LUN, selecciona una clase de almacenamiento en lugar de configurar los parámetros de forma individual. La implementación local de NetApp Console usa la clase para recomendar la ubicación más adecuada en el clúster y luego aprovisiona con los parámetros definidos en la clase.
5. **Supervisar las desviaciones en las cargas de trabajo** - la implementación local de Console evalúa continuamente cada carga de trabajo comparándola con los estándares establecidos en su clase de almacenamiento. Si se produce una desviación en la configuración o un incumplimiento de los requisitos de rendimiento, señala el problema y puede generar una alerta.
6. **Corregir la desviación para restablecer el cumplimiento** - cuando se detecta una desviación o un incumplimiento de los requisitos de rendimiento, puedes seguir los pasos guiados para corregir el problema manualmente, dejar que la implementación local de Console resuelva automáticamente las condiciones de desviación más comunes o desvincular una carga de trabajo de su clase de almacenamiento si necesitas modificar su configuración.

Cómo funcionan las clases de almacenamiento con las flotas

Las clases de almacenamiento están asociadas a flotas. Cuando asocias una clase de almacenamiento a una flota, esa clase queda disponible para todo el aprovisionamiento dentro de la flota. Esto asegura que cada carga de trabajo aprovisionada en la flota siga los mismos estándares, haciendo que las flotas sean la forma principal de aplicar un comportamiento de almacenamiento coherente en los clústeres relacionados.

Para obtener más información sobre cómo organizar flotas, consulta "Conoce la gestión de flotas en la implementación local de NetApp Console".

A dónde ir ahora

- Para comprender la organización de una flota, consulta "Conoce la gestión de flotas en la implementación local de NetApp Console".
- Para crear políticas y clases de almacenamiento, consulta "Gestiona clases y políticas de almacenamiento".
- "Provisiona almacenamiento manualmente"
- "Provisiona almacenamiento automáticamente"
- "Provisiona almacenamiento con asistencia de IA"
- Para analizar y corregir la deriva, consulta "Corrige la desviación de la clase de almacenamiento"

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

La implementación local de NetApp Console se conecta a un modelo de lenguaje a gran escala (LLM) para la gestión del almacenamiento asistida por IA. Después de la configuración, los usuarios pueden usar lenguaje natural para aprovisionar almacenamiento, investigar alertas y obtener orientación sobre almacenamiento.

> 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.

La gestión asistida por IA permite a los usuarios describir las solicitudes en lenguaje sencillo mientras que la implementación local de NetApp Console aplica tus políticas de almacenamiento.

La implementación local en la consola envía las solicitudes de LLM únicamente al endpoint que configures.

Qué puedes hacer con la gestión del almacenamiento asistida por IA

Al habilitar la integración con LLM, la implementación local de Console ofrece tres funciones a través del asistente de Console:

- **Aprovisionamiento de almacenamiento** Describe los requisitos de las cargas de trabajo en un lenguaje sencillo. La implementación local de NetApp Console recomienda y ejecuta un plan de aprovisionamiento basado en tus clases de almacenamiento.
- **Respuesta a alertas** Pídele a la implementación local de Ask Console que investigue una alerta activa. Analiza el problema y sugiere o ejecuta una acción según los permisos asignados.
- **Búsqueda y orientación** Plantea tus dudas sobre tu entorno de almacenamiento o la administración de ONTAP. La implementación local de NetApp Console ofrece respuestas contextualizadas basadas en la documentación y el estado actual del parque de equipos.

Selecciona el acceso de solo lectura o de lectura/escritura para el asistente de NetApp Console

Los usuarios eligen un modo de acceso asistente en función del resultado que quieren:

- Modo **solo lectura** para orientación e investigación sin realizar cambios en la infraestructura.
- Modo **lectura/escritura** para la ejecución guiada. La implementación local de NetApp Console muestra la acción propuesta, solicita confirmación y luego aplica el cambio.

Entiende qué controla las acciones del asistente de NetApp Console

La implementación local de NetApp Console controla las acciones del asistente de NetApp Console mediante el mismo modelo de gobernanza que se usa en toda la plataforma:

- Los controles de acceso basados en roles limitan lo que cada usuario puede ver y hacer.
- Las políticas de almacenamiento limitan el aprovisionamiento y las acciones relacionadas.
- El asistente de la consola solicita confirmación antes de ejecutar acciones que modifican el almacenamiento.

Elige una ruta de proveedor de LLM

La implementación local de NetApp Console es compatible con estos tipos de proveedores de LLM:

- **OpenAI** para acceder directamente a los modelos de OpenAI.
- **Compatible con OpenAI** para un endpoint compatible, como un gateway empresarial o un servicio de proxy.
- Anthropic para los modelos Claude de Anthropic.

La disponibilidad de los modelos depende del punto final que configures. Selecciona un modelo de la lista en el despliegue local de NetApp Console.

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".

Entiende adónde van las solicitudes de los modelos de lenguaje grande (LLM)

El flujo de datos depende de la ruta de punto final que elijas:

- Si configuras un endpoint de OpenAI, la implementación local de Console envía los prompts y el contexto al endpoint de OpenAI.
- Si configuras un endpoint compatible con OpenAI, la implementación local de Console envía los prompts y el contexto al endpoint compatible que configure tu organización.

Protege las credenciales de LLM y controla el acceso de los administradores

Protege la integración con estos controles:

- Trata la clave de la API como una credencial privilegiada y rótala según la política de tu organización.
- Revisa el uso y las alertas del lado del proveedor para detectar actividad inesperada.

Conecta tu LLM

Una vez que hayas tomado estas decisiones, continúa con "Conecta tu LLM y activa el asistente de NetApp Console".

Si fallan las comprobaciones de conexión o en tiempo de ejecución, consulta "Soluciona problemas de la integración de LLM".

Obtén más información sobre NetApp Backup and Recovery en el despliegue local de NetApp Console

NetApp Backup and Recovery es un servicio de datos que ofrece una protección de datos eficiente, segura y rentable para todas tus cargas de trabajo de ONTAP, incluidos volúmenes, bases de datos, máquinas virtuales y cargas de trabajo de Kubernetes.

Una carga de trabajo es una agrupación lógica de recursos dentro de un sistema que se gestiona como una sola unidad para protección, gobernanza, detección y recuperación. En Backup and Recovery, una carga de trabajo es la unidad que proteges. Su significado depende del origen de los datos: para Kubernetes una carga de trabajo es una aplicación, para entornos VM es una máquina virtual y para entornos de bases de datos es una base de datos.

El soporte para Backup and Recovery ya está integrado en todos los sistemas ONTAP, por lo que no necesitas hardware adicional ni gateways de medios. Esto hace que las operaciones de backup sean simples y rentables. NetApp Console simplifica la implementación de cualquier estrategia de backup, incluyendo todo el espectro de variantes de backup 3-2-1, sin necesidad de múltiples administradores de recursos o personal especializado.

> NetApp Backup and Recovery está en modo de vista previa para la implementación local de NetApp Console. El servicio aún no está disponible de forma general y las funciones y la funcionalidad están sujetas a cambios.

"Obtén más información sobre NetApp Backup and Recovery.".

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.

Función de la plataforma	Responsabilidades
"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.

Función de servicio de datos	Responsabilidades
"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.
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

Síntoma	Causa probable	Qué hay que comprobar	Próxima acción
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."

Usa la consola NetApp

Inicia sesión en NetApp Console implementación local

Puedes iniciar sesión en la implementación local de NetApp Console después de que el administrador de tu organización te haya invitado a la cuenta de usuario de la organización en Console local. Para iniciar sesión, usas la dirección de correo electrónico asociada con tu inicio de sesión.

Si inicias sesión pero no ves ningún recurso, contacta al administrador de tu organización. "Contacta al administrador de tu organización".

Pasos

1. Abre un navegador web y ve a la dirección IP donde está instalada la implementación local de NetApp Console.
2. En la página **Iniciar sesión**, introduce la dirección de correo electrónico que está asociada con tu inicio de sesión.
3. Dependiendo del método de autenticación asociado a tu inicio de sesión, se te pedirá que introduzcas tus credenciales.

   - Una cuenta de NetApp Console con tu dirección de correo electrónico y una contraseña

   > - Si la autenticación multifactorial (MFA) está activada: después de introducir tu contraseña, se te pedirá que ingreses un código TOTP (de tu sistema de autenticación) o que uses un código de recuperación.
   > - Si vas a iniciar sesión con códigos de recuperación, utilízalos en el orden que se muestra en la interfaz de usuario durante la solicitud del código de recuperación.

   +

   - Una cuenta de Active Directory con tu dirección de correo electrónico y contraseña

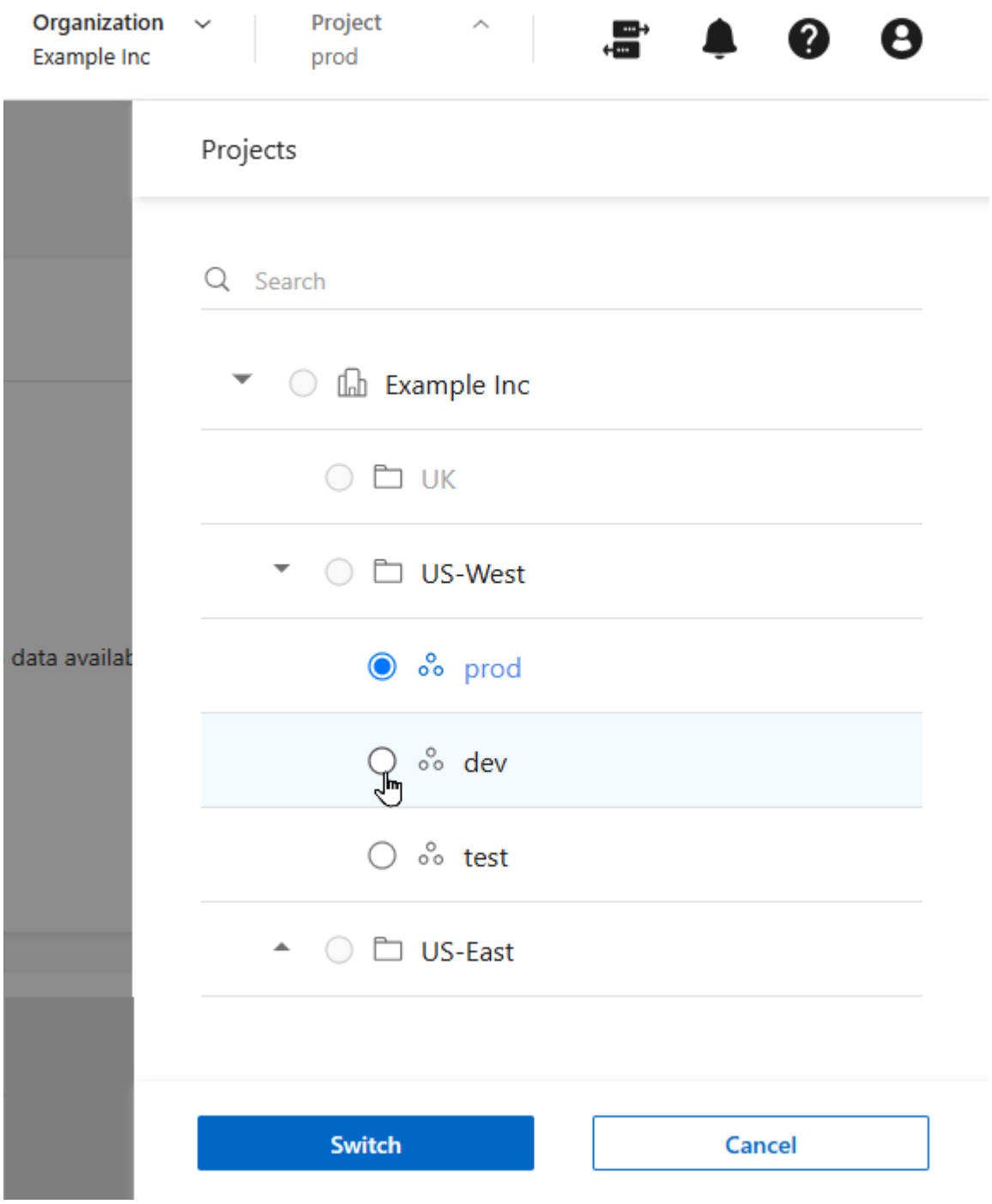
Cambia entre flotas en la implementación local de NetApp Console

En una implementación local de NetApp Console, si tienes acceso a varias flotas, puedes cambiar entre ellas en cualquier momento.

> No puedes cambiar a otra flota mientras estés viendo cualquiera de las páginas de **Identidad y acceso**.

Pasos

1. En la barra de encabezado superior de la implementación local de la Console, selecciona **Scope**.
2. Echa un vistazo a las flotas de tu organización, selecciona la flota que quieras y luego selecciona **Cambiar**.



Gestiona la configuración de usuario de tu implementación local de NetApp Console

En una implementación local de NetApp Console, puedes modificar tu perfil de implementación local de Console, incluyendo cambiar tu contraseña, habilitar la autenticación multifactor (MFA) y ver quién es tu administrador de Console.

Cambia tu nombre para mostrar

Puedes cambiar el nombre que aparece en tu implementación local de la Console, que es el que te identifica ante los demás usuarios. No puedes cambiar tu nombre de usuario ni tu dirección de correo electrónico.

Pasos

1. Selecciona el icono de perfil en la esquina superior derecha de la implementación local de la NetApp Console para ver el panel de configuración del usuario.
2. Selecciona el icono **Editar** que aparece junto a tu nombre.
3. Introduce tu nuevo nombre para mostrar en el campo **Nombre**.

Configura la autenticación multifactor

Configura la autenticación multifactor (MFA) para mejorar la seguridad exigiendo un segundo método de verificación al iniciar sesión en la implementación local de NetAppConsole.

Los usuarios que inician sesión a través del NetApp Support Site no pueden habilitar MFA. Si este es tu caso, no verás la opción para habilitar MFA en la configuración de tu perfil.

No actives la autenticación multifactor (MFA) si tu cuenta de usuario se usa para acceder a la API. La autenticación multifactor impide el acceso a la API cuando se activa para una cuenta de usuario. Usa cuentas de servicio para todo acceso a la API.

No puedes configurar la autenticación multifactor (MFA) para tu cuenta a través de la implementación local de la Console si tu cuenta utiliza Active Directory u otro servicio de directorio integrado para la autenticación.

Antes de empezar

- Ya debes haber descargado una app de autenticación, como Google Authenticator o Microsoft Authenticator, en tu dispositivo.
- Necesitarás tu contraseña para configurar la autenticación multifactor (MFA).

Si no tienes acceso a tu aplicación de autenticación o pierdes tu código de recuperación, ponte en contacto con tu administrador de la NetApp Console para que te ayude.

Pasos

1. Selecciona el icono de perfil situado en la esquina superior derecha de la Console para acceder al panel de configuración del usuario.
2. Selecciona **Configurar** junto al encabezado **Multi-Factor Authentication**.
3. Sigue las instrucciones para configurar la autenticación multifactor (MFA) en tu cuenta.
4. Cuando termines, se te pedirá que guardes tus códigos de recuperación. Elige entre copiar los códigos o descargar un archivo de texto que los contenga. Guarda estos códigos en un lugar seguro. Necesitarás los códigos de recuperación si pierdes el acceso a tu app de autenticación.

   Si necesitas iniciar sesión con un código de recuperación, utilízalos en el orden que se muestra en la interfaz de usuario durante la solicitud del código de recuperación.

   Después de configurar la autenticación multifactor (MFA), la implementación local de la Console te pedirá que introduzcas un código de un solo uso de tu aplicación de autenticación cada vez que inicies sesión.

Vuelve a generar tu código de recuperación de MFA

Solo puedes utilizar un código de recuperación una vez. Si pierdes el tuyo, genera uno nuevo.

Pasos

1. Selecciona el icono de perfil situado en la esquina superior derecha de la implementación local de la Console para acceder al panel de configuración del usuario.
2. Selecciona ••• junto al encabezado **Autenticación multifactorial**.
3. Selecciona **Regenerar código de recuperación**.
4. Copia los códigos de recuperación generados y guárdalos en un lugar seguro.

Elimina tu configuración de MFA

Eliminar la autenticación multifactor (MFA) quita el segundo paso de verificación para tu próximo inicio de sesión. Para usar MFA otra vez, tienes que configurarla de nuevo desde tus ajustes de usuario.

Si no puedes acceder a tu aplicación de autenticación o a tu código de recuperación, tendrás que ponerte en contacto con el administrador de tu organización para restablecer tu configuración de MFA.

Pasos

1. Selecciona el icono de perfil en la esquina superior derecha de la implementación local de la NetApp Console para ver el panel de configuración del usuario.
2. Selecciona ••• junto al encabezado **Autenticación multifactorial**.
3. Selecciona **Borrar**.

Ponte en contacto con el administrador de tu organización

Si necesitas ponerte en contacto con el administrador de tu organización, puedes enviarle un correo electrónico directamente desde la NetApp Console. El administrador gestiona las cuentas de usuario y los permisos dentro de tu organización.

Debes tener configurada una aplicación de correo electrónico predeterminada en tu navegador para poder utilizar la función **Contact admins**.

Pasos

1. Selecciona el icono de perfil en la esquina superior derecha de la implementación local de la NetApp Console para ver el panel de configuración del usuario.
2. Selecciona **Contact admins** para enviar un correo electrónico al administrador de tu organización.
3. Selecciona la aplicación de correo electrónico que quieras utilizar.
4. Termina el correo electrónico y selecciona **Enviar**.

Configura el modo oscuro (tema oscuro)

Puedes configurar la implementación local de NetApp Console para que se muestre en modo oscuro.

Pasos

1. Selecciona el icono de perfil en la esquina superior derecha de la implementación local de la NetApp Console para ver el panel de configuración del usuario.

2. Mueve el control deslizante **Tema oscuro** para activarlo.

Usa el asistente de NetApp Console en la implementación local de NetApp Console

Utiliza el asistente de NetApp Console en la implementación local de NetApp Console para gestionar el almacenamiento y obtener respuestas mediante lenguaje natural. Describe lo que necesitas en lenguaje sencillo, y la implementación local de NetApp Console actúa en consecuencia dentro de tus políticas de almacenamiento y acceso basado en roles.

> 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.

Las acciones del asistente están limitadas por el acceso basado en roles que se te haya asignado. "Conoce los roles de acceso".

Descubre todo lo que puedes hacer con el asistente de la consola

El asistente de la consola es una interfaz de lenguaje natural para la implementación local de NetApp Console. Haz una pregunta o describe una tarea, y te dará una respuesta o te propondrá una acción. El asistente ofrece estas capacidades:

- **Aprovisiona almacenamiento** Describe una carga de trabajo en un lenguaje sencillo. El asistente recomienda una clase de almacenamiento y una ubicación, luego crea el volumen o el LUN después de que confirmes los detalles. Por ejemplo, pídele que cree un volumen CIFS con una capacidad específica. El asistente identifica el clúster y la máquina virtual de almacenamiento (SVM), completa los parámetros necesarios y aprovisiona almacenamiento.
- **Buscar y obtener orientación** Plantea preguntas sobre tu entorno de almacenamiento, descubre las funciones de implementación local de Console y obtén respuestas contextualizadas a partir de la documentación de NetApp y del estado actual de la flota.
- **Investigar alertas** Pide al asistente que examine una alerta activa. Analiza el problema y sugiere una solución o, con tu confirmación, realiza una acción de remediación.

El asistente envía solicitudes únicamente al punto final del LLM configurado por tu administrador en la implementación local de Console. Solicita confirmación antes de realizar acciones que impliquen cambios en el almacenamiento, y todas las acciones respetan los controles de acceso basado en roles asignados a tu cuenta.

Comprueba que puedes utilizar el asistente de la consola

- Un administrador o superadministrador de la organización debe habilitar el asistente de Console conectando un modelo de lenguaje grande (LLM) a la implementación local de Console. Si no ves el botón **Asistente de Console** en el panel de control, pide a tu administrador que lo habilite. Para obtener más información, consulta "Conecta tu LLM y activa el asistente de NetApp Console".
- Asegúrate de disponer de los controles de acceso basado en roles necesarios para las acciones que deseas que realice el asistente.

Haz una pregunta al asistente de la consola o solicita una acción

Abre el asistente de la consola, elige un modo de acceso e introduce un mensaje que describa tu solicitud.

Pasos

1. Desde el panel de control de implementación local de la NetApp Console, selecciona el botón **Console assistant**.
2. Selecciona un modo de acceso:
   - Selecciona **Solo lectura** para hacer preguntas y recibir orientación sin realizar cambios.
   - Selecciona **lectura/escritura** para permitir que el asistente realice acciones en tu infraestructura de almacenamiento.
3. Escribe una frase que describa tu pregunta o tarea y, luego, selecciona **Enviar**.

   Por ejemplo: `Create a 10GiB volume for home directories named home, and share it with Everyone set to FULL_CONTROL.`
4. Revisa la respuesta del asistente:
   - Ante una pregunta, el asistente te da una respuesta que puedes poner en práctica.
   - En el caso de una acción, el asistente muestra la acción sugerida, solicita los datos que faltan, como el nivel de permiso, y luego pide confirmación antes de continuar.
5. Confirma la acción. Para operaciones asíncronas, como la creación de un volumen, el asistente crea una tarea para completar la solicitud.
6. Para consultar el estado de una solicitud, pregúntale al asistente. Por ejemplo, escribe `Let me know when the job completes`, y el asistente te mostrará el estado actual.

Gestiona el almacenamiento en NetApp Console

Conoce la gestión de flotas en la implementación local de NetApp Console

La gestión de flotas en la implementación local de NetApp Console es la práctica de organizar los sistemas de almacenamiento en grupos lógicos para que puedas aplicar políticas coherentes, controlar el acceso y supervisar el estado de los clústeres relacionados. En lugar de gestionar cada clúster de forma independiente, la gestión de flotas te permite tratar tu flota como un conjunto común de recursos para cumplir tus objetivos de almacenamiento de datos.

A medida que tu entorno de almacenamiento crece, gestionar clústeres individuales deja de ser práctico. La gestión de flotas resuelve esto dándote una forma estructurada de agrupar sistemas relacionados, delegar responsabilidades y asegurarte de que cada clúster opere bajo los mismos estándares.

Por qué es importante la gestión de flotas

La gestión de flotas aborda tres retos fundamentales:

- **Simplificación mediante la abstracción** - la gestión de flotas elimina la complejidad que supone gestionar cada infraestructura de almacenamiento por separado. En lugar de tener que ocuparte de la configuración en clúster, gestionas tu parque de almacenamiento como un todo unificado, lo que reduce la carga operativa y la fatiga decisoria.

- **Coherencia y escalabilidad** - sin una organización clara, los distintos equipos toman decisiones diferentes para cargas de trabajo similares, lo que da lugar a configuraciones fragmentadas. La gestión de flotas te permite aplicar estándares en docenas de sistemas a la vez, lo que garantiza que las nuevas cargas de trabajo partan de la misma base de referencia en todos los equipos y flotas.
- **Gobernanza y control** - a medida que los equipos crecen, necesitas límites claros sobre quién puede gestionar qué. La gestión de flotas proporciona esos límites mediante una estructura organizativa y control de acceso, asegurando que las decisiones de almacenamiento sigan estando gobernadas y sean auditables.

Cómo las flotas organizan tus recursos

La jerarquía de recursos de tu organización está formada por carpetas y flotas:

Para obtener una descripción detallada de la jerarquía y el modelo de acceso, consulta "Conoce las carpetas y las flotas en la implementación local de NetApp Console".

- **Organización** - el nivel superior que representa a tu empresa.
- **Carpetas** - te ayudan a organizar flotas relacionadas. Por ejemplo, puedes crear una carpeta para cada región o unidad de negocio, y luego crear flotas dentro de cada carpeta. Las carpetas pueden contener otras carpetas o flotas. Cuando asignas un rol a nivel de carpeta, los miembros heredan ese rol para todas las flotas dentro de la carpeta.
- **Flotas** - agrupa los sistemas de almacenamiento que gestionas. Asocias los sistemas de almacenamiento a las flotas y asignas miembros a las flotas para darles acceso.

Las carpetas son una herramienta de organización y no son visibles para los miembros que no tengan permisos de IAM, como los roles de Organization admin, Folder admin o Fleet admin. Los miembros acceden a las flotas, no a las carpetas.

Modelos habituales de organización de flotas

La forma de organizar las flotas depende de tu modelo operativo:

- **Por entorno** - crea flotas independientes para las cargas de trabajo de producción, desarrollo y prueba. Esto mantiene el almacenamiento de producción bajo políticas más estrictas, mientras permite más flexibilidad en los entornos de menor nivel.
- **Por unidad de negocio** - agrupa los clústeres que dan servicio a un departamento específico, como finanzas, ingeniería o recursos humanos, en una flota dedicada. Luego puedes asignar responsabilidades de gestión del almacenamiento a los miembros del equipo de esa unidad de negocio sin exponerles a otras flotas.
- **Por ubicación o centro de datos** - cuando los clústeres están distribuidos entre distintos emplazamientos, organizarlos por ubicación te permite supervisar el estado a nivel de emplazamiento, aplicar políticas específicas para cada región y realizar un seguimiento del consumo de capacidad por emplazamiento.
- **Por nivel de aplicación** - agrupa los clústeres que alojan un tipo específico de carga de trabajo, como bases de datos, recursos compartidos de archivos o máquinas virtuales, para que puedas aplicar normas coherentes y adaptadas a ese tipo de carga de trabajo en toda la flota.

Utiliza carpetas para añadir otro nivel de organización. Por ejemplo, crea una carpeta para cada región y luego crea flotas por entorno dentro de cada carpeta regional.

Cómo la gestión de flotas facilita el control de acceso

Las flotas y las carpetas sirven para delimitar el acceso de los usuarios y las responsabilidades administrativas:

- **Acceso a nivel de carpeta** - cuando asignas un rol a nivel de carpeta, el miembro hereda ese rol para todas las flotas y recursos dentro de la carpeta. Esto te permite delegar responsabilidades administrativas sin conceder acceso a toda la organización.
- **Acceso a nivel de flota** - cuando asignas un rol a nivel de flota, el miembro solo tiene acceso a los sistemas de almacenamiento dentro de esa flota. Esto te permite delegar la gestión del almacenamiento a miembros del equipo o a responsables de aplicaciones sin exponer partes no relacionadas de tu infraestructura.

La implementación local de la consola permite la supervisión del estado y el rendimiento a nivel de flota, así puedes ver el estado de todos los clústeres de una flota desde una sola vista, identificar problemas temprano y actuar antes de que afecten a las cargas de trabajo.

Cómo funciona la gestión del almacenamiento

La gestión del almacenamiento consiste en definir normas de almacenamiento, aplicarlas de forma coherente y gestionar las cargas de trabajo para que se mantengan alineadas a lo largo del tiempo. En la implementación local de Console, dichas normas se expresan como políticas de clase de almacenamiento y clases de almacenamiento, se aplican a flotas y se hacen cumplir mediante flujos de trabajo de aprovisionamiento regidos por RBAC y el registro de auditoría.

La implementación local de NetApp Console integra cuatro conceptos en un único flujo de trabajo:

- Las **flotas** definen el ámbito en el que gestionas el almacenamiento. Una flota agrupa sistemas para que puedas controlar el acceso, aplicar normas de forma coherente y gestionar los recursos como una unidad.
- Las **políticas de clase de almacenamiento** definen los estándares como módulos reutilizables (rendimiento, capacidad, seguridad, protección de datos).
- **Las clases de almacenamiento** expresan la finalidad de la carga de trabajo. Una clase de almacenamiento es una plantilla con nombre compuesta por una o más políticas.
- **Los flujos de trabajo de aprovisionamiento** crean almacenamiento dentro de unos límites preestablecidos. Los distintos flujos de trabajo toman decisiones de configuración de forma diferente, pero todos pueden aplicar clases de almacenamiento y siguen estando gobernados por RBAC y el registro de auditoría.

Enfoques de aprovisionamiento

La implementación local de NetApp Console admite tres métodos de aprovisionamiento, todos ellos regulados por RBAC, el registro de auditoría y las normas de clase de almacenamiento:

- **Aprovisionamiento manual** - Tú seleccionas el sistema de destino y especificas directamente los detalles de configuración. Usa esto cuando necesites un control explícito sobre la selección y la configuración del sistema.
- **Aprovisionamiento automatizado** - tú proporcionas los datos de la carga de trabajo y, si lo deseas, seleccionas una clase de almacenamiento. La implementación local de NetApp Console recomienda la ubicación más adecuada y aplica ajustes basados en las clases para reducir las decisiones manuales.
- **Aprovisionamiento asistido por IA (agente)**: describes lo que necesitas en lenguaje natural. La implementación local de NetApp Console propone un plan sujeto a las restricciones de RBAC y clases de almacenamiento, y solo realiza el aprovisionamiento después de que lo revises y apruebes.

A dónde ir ahora

- Para conocer las normas de almacenamiento, consulta "Obtén información sobre las clases de almacenamiento y las políticas en el despliegue local de NetApp Console".
- Para crear y gestionar flotas, consulta "Gestiona carpetas y flotas".
- "Provisiona almacenamiento manualmente"
- "Provisiona almacenamiento automáticamente"
- "Provisiona almacenamiento con asistencia de IA"

Estandariza el comportamiento del almacenamiento

Obtén información sobre las clases de almacenamiento y las políticas en el despliegue local de NetApp Console

Una clase de almacenamiento es una plantilla reutilizable que define cómo debe comportarse el almacenamiento. Cuando aprovisionas almacenamiento utilizando una clase de almacenamiento, NetApp Console local deployment aplica automáticamente los estándares codificados en esa clase sin que los administradores tengan que tomar decisiones de configuración individuales para cada carga de trabajo.

Las clases de almacenamiento se crean a partir de políticas de clases de almacenamiento, que definen aspectos concretos del comportamiento del almacenamiento. En conjunto, te permiten definir los estándares de almacenamiento de tu organización una sola vez y aplicarlos de forma coherente en todas las flotas.

Qué son las políticas de clase de almacenamiento

Una política de clase de almacenamiento define una dimensión del comportamiento del almacenamiento. Las políticas son elementos básicos reutilizables que combinas para crear clases de almacenamiento.

Entre los tipos de políticas más comunes se incluyen:

- **Políticas de rendimiento** - define los objetivos de latencia, las IOPS o los requisitos de rendimiento.
- **Políticas de capacidad** - define el modo de aprovisionamiento, las alertas de umbrales o los límites de crecimiento.
- **Políticas de seguridad** - define requisitos de cifrado, cumplimiento o control de acceso.
- **Políticas de protección de datos** - define las programaciones de snapshots, los destinos de replicación o los períodos de retención.

Defines las políticas de forma independiente y luego las combinas cuando creas una clase de almacenamiento. Esto te permite reutilizar la misma política de rendimiento en varias clases, o actualizar una política de capacidad en un solo lugar y aplicar ese cambio a todas las clases que la usan.

Qué son las clases de almacenamiento

Una clase de almacenamiento es una plantilla con nombre que se compone de una o varias políticas. Refleja los estándares de almacenamiento de tu organización para un tipo específico de carga de trabajo.

Por ejemplo, podrías crear una clase de almacenamiento **Production Database** que combine alto rendimiento, alta disponibilidad y políticas estrictas de protección de datos, o una clase de almacenamiento **Development File Share** que combine rendimiento moderado, capacidad flexible y políticas básicas de protección de datos.

Los administradores de almacenamiento definen clases de almacenamiento para plasmar los requisitos de la empresa. Toda la actividad de aprovisionamiento, ya sea manual, a través de flujos de trabajo guiados o mediante automatización, se basa en la biblioteca de clases que han aprobado esos administradores.

Cómo las clases de almacenamiento garantizan el cumplimiento de las normas

Cuando aprovisionas almacenamiento, seleccionas una clase de almacenamiento en lugar de configurar parámetros individuales. La implementación local de NetApp Console utiliza las políticas de esa clase para identificar qué clústeres de tu flota tienen la capacidad y el margen de rendimiento necesarios para soportar la carga de trabajo, recomendar la mejor opción de ubicación y aplicar automáticamente los ajustes definidos por la clase en el momento del aprovisionamiento.

Tras el aprovisionamiento, la implementación local de Console evalúa continuamente cada carga de trabajo en función de los estándares de su clase de almacenamiento.

Desviación de la clase de almacenamiento y cumplimiento

Cuando una carga de trabajo deja de ajustarse a la finalidad de su clase de almacenamiento, la implementación local de Console la marca para su investigación y corrección.

Los problemas se dividen en dos categorías:

- **Desviación de la configuración**: Los parámetros de almacenamiento regulados por la política de clase de almacenamiento ya no se corresponden con la configuración prevista. Esto puede ocurrir cuando se realizan cambios directamente en el clúster ONTAP o fuera de los flujos de trabajo estándar de aprovisionamiento de almacenamiento.
- **Incumplimiento de los requisitos de rendimiento**: El comportamiento en tiempo de ejecución de la carga de trabajo ya no cumple con la intención de rendimiento de la clase de almacenamiento (por ejemplo, una presión sostenida cerca de un límite de QoS o una latencia de cola elevada).

Una vista de análisis explica qué ha cambiado y por qué. Es posible que haya disponibles acciones de corrección guiadas (por ejemplo, **Fix it**) para ayudar a restablecer el cumplimiento. Algunas correcciones se pueden aplicar directamente, mientras que otras pueden requerir alinear la carga de trabajo a una clase de almacenamiento diferente para restablecer el comportamiento previsto.

Dónde investigar

Normalmente, puedes investigar las desviaciones y los incumplimientos desde una de estas ubicaciones (la disponibilidad depende de tu implementación y permisos):

- **Clases de almacenamiento:** Drift / Compliance
- **Alertas:** Analiza

Para obtener instrucciones paso a paso, consulta Corrige la desviación de la clase de almacenamiento.

Flujo de trabajo de principio a fin

Los pasos siguientes describen el proceso para utilizar las clases de almacenamiento con el fin de estandarizar y gestionar el almacenamiento en tu entorno:

1. **Crear políticas de clases de almacenamiento -** las políticas definen los distintos aspectos del comportamiento del almacenamiento (objetivos de rendimiento, ajustes de capacidad, requisitos de seguridad, calendarios de protección de datos). Crea las políticas antes de crear una clase de almacenamiento.

2. **Crear una clase de almacenamiento** - configura una clase de almacenamiento combinando una política de cada categoría aplicable. Puedes utilizar una clase de almacenamiento predefinida o crear una personalizada que se ajuste a las normas de tu organización.
3. **Asocia la clase de almacenamiento con una flota** - después de crear una clase de almacenamiento, asóciala a la flota donde se usará para el aprovisionamiento de almacenamiento y la supervisión del cumplimiento.
4. **Aprovisiona almacenamiento usando la clase de almacenamiento** - Cuando aprovisiones un volumen o LUN, selecciona una clase de almacenamiento en lugar de configurar los parámetros de forma individual. La implementación local de NetApp Console usa la clase para recomendar la ubicación más adecuada en el clúster y luego aprovisiona con los parámetros definidos en la clase.
5. **Supervisar las desviaciones en las cargas de trabajo** - la implementación local de Console evalúa continuamente cada carga de trabajo comparándola con los estándares establecidos en su clase de almacenamiento. Si se produce una desviación en la configuración o un incumplimiento de los requisitos de rendimiento, señala el problema y puede generar una alerta.
6. **Corregir la desviación para restablecer el cumplimiento** - cuando se detecta una desviación o un incumplimiento de los requisitos de rendimiento, puedes seguir los pasos guiados para corregir el problema manualmente, dejar que la implementación local de Console resuelva automáticamente las condiciones de desviación más comunes o desvincular una carga de trabajo de su clase de almacenamiento si necesitas modificar su configuración.

Cómo funcionan las clases de almacenamiento con las flotas

Las clases de almacenamiento están asociadas a flotas. Cuando asocias una clase de almacenamiento a una flota, esa clase queda disponible para todo el aprovisionamiento dentro de la flota. Esto asegura que cada carga de trabajo aprovisionada en la flota siga los mismos estándares, haciendo que las flotas sean la forma principal de aplicar un comportamiento de almacenamiento coherente en los clústeres relacionados.

Para obtener más información sobre cómo organizar flotas, consulta "Conoce la gestión de flotas en la implementación local de NetApp Console".

A dónde ir ahora

- Para comprender la organización de una flota, consulta "Conoce la gestión de flotas en la implementación local de NetApp Console".
- Para crear políticas y clases de almacenamiento, consulta "Gestiona clases y políticas de almacenamiento".
- "Provisiona almacenamiento manualmente"
- "Provisiona almacenamiento automáticamente"
- "Provisiona almacenamiento con asistencia de IA"
- Para analizar y corregir la deriva, consulta "Corrige la desviación de la clase de almacenamiento"

Comprender las políticas de clase de almacenamiento en la implementación local de NetApp Console

Las políticas de clase de almacenamiento son los componentes básicos que usas para crear una clase de almacenamiento. Cada política controla un aspecto específico del comportamiento del almacenamiento. Cuando combinas políticas en una clase de almacenamiento, creas una plantilla reutilizable que la implementación local de la NetApp Console aplica automáticamente al momento de aprovisionar y supervisa de forma continua durante todo el ciclo de vida de una carga de trabajo.

Las políticas como bloques de construcción

Una clase de almacenamiento se compone de una o más políticas, cada una de las cuales regula una dimensión diferente del comportamiento del almacenamiento. Los administradores de almacenamiento definen políticas para plasmar los estándares de la empresa—expectativas de rendimiento, umbrales de capacidad, reglas de ubicación de los datos—y luego agrupan esas políticas en plantillas de clases de almacenamiento. Cuando se aprovisiona una carga de trabajo utilizando una clase de almacenamiento, hereda todas las políticas de esa clase. Este diseño separa la responsabilidad de definir los estándares del acto de aprovisionamiento, así el almacenamiento puede aprovisionarse de forma coherente mediante flujos de trabajo automatizados sin necesidad de tomar decisiones de configuración individuales.

Tipos de políticas de clase de almacenamiento

NetApp Console la implementación local incluye cuatro tipos de políticas que puedes utilizar para crear clases de almacenamiento:

Política de rendimiento

Una política de rendimiento establece los IOPS/TB esperados, los IOPS/TB máximos, los IOPS mínimos absolutos y los objetivos de latencia esperados para una carga de trabajo. La implementación local de NetApp Console utiliza estos valores para recomendar clústeres con suficiente margen al momento del aprovisionamiento y para detectar desviaciones en los IOPS o la latencia después del aprovisionamiento.

Política de capacidad

Una política de capacidad controla cómo un volumen consume y gestiona el espacio. Establece la reserva de espacio (thick, thin o la predeterminada del sistema), el comportamiento de crecimiento automático, la organización en niveles de FabricPool y si las cargas de trabajo NAS deben aprovisionarse como volúmenes FlexVol o FlexGroup.

Política de seguridad

Una política de seguridad establece los requisitos de cifrado, protección contra ransomware y FIPS para una carga de trabajo. Cada atributo puede configurarse con un valor obligatorio o dejarse como "cualquiera" para aceptar el valor predeterminado del sistema.

Política de protección de datos

Una política de protección de datos establece el número de instantáneas que se conservan en cada intervalo para garantizar que las cargas de trabajo que utilizan dicha política cuenten con un programa de copias de seguridad coherente.

Políticas predeterminadas

La implementación local de Console incluye políticas definidas por el sistema para los cuatro tipos de políticas. Puedes utilizar estas políticas tal cual al crear una clase de almacenamiento o copiarlas como punto de partida para crear políticas personalizadas que se adapten a los requisitos de tu organización.

Políticas de rendimiento

Nombre	Tipo	IOPS previstas por TB	IOPS máximas por TB	Mínimo absoluto de IOPS	Latencia prevista (ms)	Resumen
Extreme para datos de bases de datos	Definido por el sistema	12.288	24.576	2.000	1	Úsalo para volúmenes de datos de bases de datos transaccionales que requieren IOPS altos y sostenidos y una latencia inferior al milisegundo.
Extreme para registros de bases de datos	Definido por el sistema	22.528	45.056	4.000	1	Úsalo para los volúmenes de registro de transacción de base de datos que requieren el nivel mínimo más alto de IOPS para evitar cuellos de botella en la escritura.
Extreme para datos compartidos de base de datos	Definido por el sistema	16.384	32.768	2.000	1	Úsalo para volúmenes de bases de datos compartidos a los que acceden varios hosts y que requieren un alto rendimiento y una latencia constante.
Rendimiento extremo	Definido por el sistema	6.144	12.288	1.000	1	Úsalo para cargas de trabajo de HPC, IA/ML y análisis que requieren altos picos de IOPS y una latencia baja y predecible.
Rendimiento	Definido por el sistema	2.048	4.096	500	2	Úsalo para aplicaciones virtualizadas y empresariales que requieren un rendimiento fiable sin demandas extremas de IOPS.
Valor	Definido por el sistema	128	512	75	17	Úsalo para cargas de trabajo sensibles al coste, como directorios personales, recursos compartidos de archivos y archivos.

Políticas de capacidad

Nombre	Tipo	Reserva de espacio	Modo Autogrow	Política de tiering	Tipo de volumen (NAS)	Resumen
por defecto	Definido por el sistema	Valor predeterminado del sistema	Valor predeterminado del sistema	ninguna	Valor predeterminado del sistema	Úsalo para cargas de trabajo generales en las que el comportamiento predeterminado de la plataforma en cuanto a capacidad resulte aceptable.

Nombre	Tipo	Reserva de espacio	Modo Autogrow	Política de tiering	Tipo de volumen (NAS)	Resumen
producción	Definido por el sistema	Valor predeterminado del sistema	crecer	ninguna	Valor predeterminado del sistema	Úsalo para cargas de trabajo de producción que deban ampliarse automáticamente para evitar fallos por falta de espacio.

Políticas de seguridad

Nombre	Tipo	Cifrado	Protección contra ransomware	FIPS	Resumen
por defecto	Definido por el sistema	cualquier	cualquier	cualquier	Utilízalo para cargas de trabajo donde el comportamiento de seguridad predeterminado de la plataforma sea aceptable.
anti-ransomware	Definido por el sistema	cualquier	en	cualquier	Úsalo para cargas de trabajo que contengan datos confidenciales o datos críticos para el negocio y que requieran protección activa contra el ransomware.
producción	Definido por el sistema	habilitado	cualquier	cualquier	Úsalo para cargas de trabajo de producción donde se requiera el cifrado para el cumplimiento.

Políticas de protección de datos

Nombre	Tipo	Instantáneas por hora	Instantáneas diarias	Instantáneas semanales	Instantáneas mensuales	Resumen
por defecto	Definido por el sistema	6	2	2	0	Úsalo para cargas de trabajo estándar que requieren puntos de recuperación a corto plazo sin la sobrecarga de retención a largo plazo.
3 meses - por horas	Definido por el sistema	23	6	4	3	Úsalo para cargas de trabajo reguladas o críticas para el negocio que requieren puntos de recuperación intradía granulares y una retención histórica de tres meses.

Revisa las políticas de clase de almacenamiento predefinidas en la implementación local de NetApp Console

La implementación local de NetApp Console incluye políticas definidas por el sistema para los cuatro tipos de políticas. Utiliza esta referencia para identificar qué política se adapta mejor a los requisitos de tu carga de trabajo a la hora de crear o personalizar una clase de almacenamiento.

Políticas de rendimiento

Rendimiento extremo

Úsalo para cargas de trabajo de HPC, IA/ML y análisis que requieren altos picos de IOPS y una latencia baja y predecible.

Extreme para datos de bases de datos

Úsalo para volúmenes de datos de bases de datos transaccionales que requieren IOPS altos y sostenidos y una latencia inferior al milisegundo.

Extreme para registros de bases de datos

Úsalo para los volúmenes de registro de transacción de base de datos que requieren el nivel mínimo más alto de IOPS para evitar cuellos de botella en la escritura.

Extreme para datos compartidos de base de datos

Úsalo para volúmenes de bases de datos compartidos a los que acceden varios hosts y que requieren un alto rendimiento y una latencia constante.

Rendimiento

Úsalo para aplicaciones virtualizadas y empresariales que requieren un rendimiento fiable sin demandas extremas de IOPS.

Valor

Úsalo para cargas de trabajo sensibles al coste, como directorios personales, recursos compartidos de archivos y archivos.

Políticas de capacidad

Capacidad de autogrowth

Úsalo para cargas de trabajo de producción que deban ampliarse automáticamente para evitar fallos por falta de espacio.

Políticas de seguridad

Cifrado en reposo

Úsalo para cargas de trabajo de producción donde se requiera el cifrado para el cumplimiento.

Protección contra ransomware

Úsalo para cargas de trabajo que contengan datos confidenciales o datos críticos para el negocio y que requieran protección activa contra el ransomware.

Seguridad estándar

Utilízalo para cargas de trabajo donde el comportamiento de seguridad predeterminado de la plataforma sea aceptable.

Políticas de protección de datos

por defecto

Úsalo para cargas de trabajo estándar que requieren puntos de recuperación a corto plazo sin la sobrecarga de retención a largo plazo.

3 meses - por horas

Úsalo para cargas de trabajo reguladas o críticas para el negocio que requieren puntos de recuperación intradía granulares y tres meses de retención histórica.

Recuperación de 30 días

Úsalo para cargas de trabajo estándar que requieren puntos de recuperación a corto plazo sin la sobrecarga de retención a largo plazo.

Recuperación de 90 días

Úsalo para cargas de trabajo reguladas o críticas para el negocio que requieren puntos de recuperación intradía granulares y tres meses de retención histórica.

Crea clases de almacenamiento en el despliegue local de NetApp Console

Crea una clase de almacenamiento en la implementación local de la NetApp Console para estandarizar la forma en que se aprovisiona y gobierna el almacenamiento en todas tus flotas. Una clase de almacenamiento es una plantilla reutilizable que agrupa políticas de clase de almacenamiento, como objetivos de rendimiento, comportamiento de la capacidad, requisitos de seguridad y programaciones de protección de datos, en una única definición con nombre.

Cuando los usuarios (o la automatización) aprovisionan un volumen o un LUN utilizando una clase de almacenamiento, NetApp Console local deployment aplica automáticamente las políticas de dicha clase. Después del aprovisionamiento, Console local deployment supervisa continuamente las cargas de trabajo en relación con la clase de almacenamiento para detectar desviaciones y puede guiarte o automatizar la corrección para restablecer el cumplimiento.

Antes de empezar

- Detecta al menos un clúster ONTAP para que la implementación local de Console tenga destinos para las recomendaciones de ubicación.
- Asegúrate de que tienes el rol de Organization admin (o un rol que te otorgue permisos para gestionar las clases de almacenamiento en tu entorno).
- Crea (o identifica) las políticas de clase de almacenamiento que planeas usar—rendimiento, capacidad, seguridad y protección de datos— porque las clases de almacenamiento se ensamblan a partir de políticas.

Crear una clase de almacenamiento

Debes tener el rol de Organization admin, Folder o fleet admin para añadir una clase de almacenamiento.

Pasos

1. Selecciona **Storage > Management**.
2. Selecciona **Clases de almacenamiento**.

3. Selecciona **Add**.
4. En el apartado **Información básica**, introduce lo siguiente:
   - **Nombre de la clase de almacenamiento**: Introduce un nombre único para la clase de almacenamiento.
   - **Descripción**: (Opcional) Introduce una descripción de la clase de almacenamiento.
   - **Aplicaciones recomendadas**: (Opcional) introduce una lista de aplicaciones recomendadas para la clase de almacenamiento.
5. En **Políticas de almacenamiento**, selecciona una o varias políticas para asociar con la clase de almacenamiento.
6. Selecciona **Add**.

Personaliza una clase de almacenamiento existente

Debes tener el rol de Organization admin o Folder o fleet admin para personalizar una clase de almacenamiento existente.

Pasos

1. Selecciona **Storage > Management**.
2. Selecciona **Clases de almacenamiento**.
3. Para la clase de almacenamiento que quieras personalizar, selecciona **…** y, a continuación, selecciona **Duplicar**.
4. En la sección **Información básica**, actualiza lo siguiente según sea necesario:
   - **Nombre de la clase de almacenamiento**: Introduce un nombre único para la clase de almacenamiento.
   - **Descripción**: (Opcional) Introduce una descripción de la clase de almacenamiento.
   - **Aplicaciones recomendadas**: (Opcional) introduce una lista de aplicaciones recomendadas para la clase de almacenamiento.
5. En **Políticas de almacenamiento**, selecciona una o varias políticas para asociar con la clase de almacenamiento.
6. Selecciona **Add**.

Editar una clase de almacenamiento definida por el usuario

Debes tener el rol de Organization admin, Folder admin o fleet admin para editar una clase de almacenamiento definida por el usuario.

Pasos

1. Selecciona **Storage > Management**.
2. Selecciona **Clases de almacenamiento**.
3. Para la clase de almacenamiento que quieras editar, selecciona **…** y luego selecciona **Editar**.
4. En **Información básica**, edita lo siguiente según sea necesario:
   - **Nombre de la clase de almacenamiento**: Introduce un nombre único para la clase de almacenamiento.
   - **Descripción**: (Opcional) Introduce una descripción de la clase de almacenamiento.

- **Aplicaciones recomendadas**: (Opcional) introduce una lista de aplicaciones recomendadas para la clase de almacenamiento.

5. En **Políticas de almacenamiento**, selecciona una o varias políticas para asociar con la clase de almacenamiento.
6. Selecciona **Editar**.

Eliminar una clase de almacenamiento definida por el usuario

Debes tener el rol de administrador de la organización, de carpetas o de flota para eliminar una clase de almacenamiento definida por el usuario.

Pasos

1. Selecciona **Storage > Management**.
2. Selecciona **Clases de almacenamiento**.
3. Para la clase de almacenamiento que quieras eliminar, selecciona **…** y luego selecciona **Eliminar**.
4. Selecciona **Borrar**.

   Ten en cuenta que esta acción no se puede deshacer. Si eliminas una clase de almacenamiento que se está utilizando actualmente, los volúmenes o LUNs aprovisionados con esa clase seguirán funcionando pero ya no estarán asociados con la clase eliminada.

Aprovisiona almacenamiento en la implementación local de NetApp Console

Aprovisiona volúmenes y LUN en la implementación local de NetApp Console para que los recursos de almacenamiento estén disponibles para tus cargas de trabajo. Durante el aprovisionamiento, puedes seleccionar opcionalmente una clase de almacenamiento para aplicar políticas de almacenamiento predefinidas y normas de la organización.

Roles de acceso necesarios

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

Aprovisiona un volumen

Pasos

1. Selecciona **Storage > Management**.
2. Selecciona **Fleets**.
3. Selecciona la flota en la que quieres aprovisionar.
4. Selecciona **Add**.
5. En el menú, selecciona **Volume**.
6. En la sección **Detalles del volumen**:
   a. Introduce un nombre para el volumen.
   b. Introduce la capacidad (y selecciona las unidades si es necesario).
   c. (Opcional) Selecciona una clase de almacenamiento para aplicar las políticas de clase de almacenamiento. Si no seleccionas una, el volumen se aprovisiona sin políticas de clase de almacenamiento.

7. En **Detalles del sistema**:
    a. Selecciona un sistema de entre los sistemas elegibles para la flota seleccionada.
    b. Selecciona una máquina virtual de almacenamiento.
8. En **Detalles del host (NAS)**, elige cómo los hosts acceden al volumen:
    a. Exportación mediante NFS (las políticas de exportación controlan qué hosts NFS pueden acceder al volumen)
    b. Compartir mediante SMB/CIFS
9. Selecciona **Add**.

Aprovisionar un LUN

Pasos

1. Selecciona **Storage > Management**.
2. Selecciona **Fleets**.
3. Selecciona la flota en la que quieres aprovisionar.
4. Selecciona **Add**.
5. En el menú, selecciona **LUNs**.
6. En la sección **Detalles de almacenamiento LUN**:
    a. Introduce un nombre de prefijo.
    b. Introduce el número de LUNs que deseas crear con ese prefijo.
    c. Introduce la capacidad por LUN (y selecciona las unidades si es necesario).
    d. (Opcional) Selecciona una clase de almacenamiento para aplicar las políticas de clase de almacenamiento. Si no seleccionas una, los LUN se aprovisionan sin políticas de clase de almacenamiento.
7. En **Detalles del sistema**:
    a. Selecciona un sistema (si se te solicita).
    b. Selecciona una máquina virtual de almacenamiento.
8. En **Detalles del host (SAN)**, elige cómo los hosts acceden al volumen:
    a. Selecciona el sistema operativo del host (por ejemplo, Windows o Linux) para establecer los valores predeterminados recomendados para la alineación de LUN y el tamaño de bloque.
    b. Selecciona el grupo de asignación de hosts para controlar qué iniciadores pueden acceder a los LUNs.
9. Selecciona **Add**.

Supervisa el estado del almacenamiento

Supervisión del almacenamiento en la implementación local de NetApp Console

NetApp Console la implementación local te ayuda a supervisar el almacenamiento en todas las flotas con paneles, alertas, análisis detallados y medidas correctivas, para que puedas detectar y resolver problemas antes de que afecten las cargas de trabajo.

Supervisa el estado de toda la flota mediante paneles de control

Empieza por los paneles de control para obtener una visión rápida del estado y el rendimiento del almacenamiento. Utiliza la página de inicio para consultar las métricas de un vistazo, abre la tabla de paneles de control para acceder a los paneles predefinidos y personalizados, y pasa a las alertas, la investigación y la corrección cuando necesites más detalles.

- "Ver las métricas de la página de inicio en NetApp Console en una implementación local"
- "Mantén los paneles actualizados en la implementación local de NetApp Console"
- "Conoce los paneles personalizados en la implementación local de NetApp Console"

Investiga problemas de rendimiento

Utiliza el Workload Analyzer para investigar problemas de rendimiento en volúmenes concretos. Correlaciona la latencia, el rendimiento, las IOPS y los cambios de configuración para que puedas identificar las causas raíz.

- "Obtén información sobre el Workload Analyzer de la implementación local de NetApp Console"
- "Investiga la alta latencia en un volumen en una implementación local de NetApp Console"
- "Investiga la demanda de alto rendimiento en un volumen en una implementación local de NetApp Console"
- "Aprende sobre las métricas de Workload Analyzer en el despliegue local de NetApp Console"

Configura alertas y notificaciones

Configura las políticas de alertas y los canales de notificación para que las personas adecuadas se enteren de las condiciones de almacenamiento que requieren atención. Por ejemplo, dirige una advertencia de capacidad al equipo de almacenamiento y una alerta de protección al backup admin que puede actuar en consecuencia.

"Configura las notificaciones y las políticas de alerta en el despliegue local de NetApp Console". "Visualiza las alertas de almacenamiento en el despliegue local de NetApp Console".

Soluciona problemas

Cuando detectes un problema, soluciona directamente desde NetApp Console implementación local:

- **Corrección automática** — La implementación local de NetApp Console aplica medidas correctivas automáticamente según reglas predefinidas.
- **Solución guiada** — Sigue las recomendaciones paso a paso para resolver problemas con pleno control sobre cada acción.

Supervisión mediante paneles de control

Ver las métricas de la página de inicio en NetApp Console en una implementación local

Utiliza el panel de control de la página de inicio en la implementación local de NetApp Console como tu punto de partida predeterminado para supervisar el estado y el rendimiento del almacenamiento. Ofrece métricas a grandes rasgos sobre el estado de la flota, alertas, seguridad, uso de la capacidad, latencia, rendimiento y IOPS.

El panel de control de la página de inicio se limita automáticamente solo a las flotas y sistemas que estás

autorizado a ver. También puedes añadir un panel de control personalizado a la página de inicio para el monitoreo específico de tu rol.

Utiliza las tarjetas como un flujo de trabajo de clasificación por niveles. Empieza por **Fleet health** y **Alerts** para detectar puntos de riesgo. Utiliza **System health status** y **Recommended remediations** para identificar los recursos afectados. Utiliza **Capacity usage**, **Latency**, **Throughput** e **IOPS** para investigar las causas raíz.

Estado de la flota

La ficha **Estado de la flota** muestra un resumen a grandes rasgos del estado de las cinco principales flotas, incluyendo el número de sistemas, la capacidad utilizada, el cumplimiento de las normas de seguridad y las alertas críticas. Utiliza esta ficha para identificar qué flotas requieren atención inmediata. Selecciona el nombre de la flota para ver un panel de control específico de la flota seleccionada.

Medidas correctivas recomendadas

La ficha **Medidas correctivas recomendadas** recoge los problemas activos y las acciones sugeridas. La ficha prioriza las medidas correctivas en función de la presión sobre la capacidad, los recursos fuera de línea y los riesgos relacionados con la protección.

Alertas

La ficha **Alertas** resume el volumen de alertas en el intervalo de tiempo seleccionado y las agrupa por gravedad. Utiliza esta ficha para conocer la carga actual de incidentes y detectar cambios recientes en las alertas críticas, de advertencia o informativas.

Seguridad

La ficha **Seguridad** resume los indicadores de cumplimiento y protección, como el cumplimiento del sistema y los controles relacionados con el ransomware. Utiliza esta vista para supervisar las tendencias de seguridad en todos tus recursos.

Uso de la capacidad

La ficha **Uso de la capacidad** muestra las tendencias de uso previstas e históricas en las flotas o sistemas seleccionados. Usa esta ficha para identificar patrones de crecimiento y planificar capacidad adicional.

Latencia

La tarjeta **Latencia** muestra la evolución del tiempo de respuesta a lo largo del tiempo en los sistemas seleccionados. Utiliza esta tendencia para detectar retrasos de rendimiento incipientes y comparar la latencia relativa entre los distintos recursos.

Rendimiento

La ficha **Throughput** muestra las tasas de transferencia de datos a lo largo del tiempo para los sistemas seleccionados. Utiliza esta ficha para comprender la intensidad de la carga de trabajo y supervisar los cambios en la demanda de throughput.

IOPS

La tarjeta **IOPS** muestra las tasas de operaciones de entrada/salida a lo largo del tiempo. Utiliza esta tarjeta para comparar los niveles de actividad entre sistemas e identificar la demanda de E/S sostenida o intermitente.

Tarjeta del panel de control (ejemplo de tarjeta de métricas)

La zona inferior del **Dashboard** puede mostrar un dashboard personalizado seleccionado por el usuario, como la latencia media de un ámbito de producción concreto. Utiliza estas tarjetas para realizar un seguimiento específico por equipo, carga de trabajo u objetivo.

Estado de salud del sistema

La ficha **Estado de salud del sistema** muestra una lista de los sistemas individuales junto con su estado de salud actual. Utiliza esta ficha para identificar rápidamente los sistemas que no funcionan correctamente y relacionar los cambios de estado con las alertas y las señales de rendimiento.

Información relacionada

- "Conoce los paneles personalizados en la implementación local de NetApp Console"
- "Conoce las tarjetas personalizadas del panel y las métricas en la implementación local de NetApp Console"

Usa paneles personalizados

Conoce los paneles personalizados en la implementación local de NetApp Console

Utiliza los paneles personalizados en NetApp Console en una implementación local para crear vistas de supervisión enfocadas para equipos, flotas, cargas de trabajo y objetivos operativos concretos. Los paneles personalizados complementan el panel de la página de inicio al añadir visibilidad específica a la supervisión general siempre disponible.

Cómo funcionan juntos los distintos tipos de paneles de control

Panel de control de la página de inicio
: Paneles de supervisión listos para usar sobre capacidad, alertas, capacidad de rendimiento, licencias y estado de la protección de datos. Las vistas están preconfiguradas y se actualizan automáticamente. "Ver las métricas de la página de inicio en NetApp Console en una implementación local".

Paneles de control personalizados
: Vistas de supervisión específicas para cada función, creadas a partir de tarjetas predefinidas, que incluyen ámbito, métricas, recursos de destino y ventanas de tiempo seleccionables.

Utilízalas ambas a la vez: * Empieza en la página de inicio para el seguimiento diario de los valores de referencia. * Usa los paneles personalizados para investigar de forma específica por equipo, flota, carga de trabajo o pregunta operativa.

Solo puedes añadir un panel de control personalizado a la página de inicio a la vez.

Entiende los paneles personalizados

Un panel personalizado es una colección guardada de tarjetas que tú organizas en una cuadrícula. Cada tarjeta se basa en una plantilla predefinida con una métrica y un tipo de gráfico. Cuando añades una tarjeta, configuras el alcance, los objetos de destino, la agregación y la ventana temporal.

Los paneles y las fichas personalizados son privados para ti. Cada ficha muestra datos solo de los recursos de almacenamiento que estás autorizado a ver.

Puedes eliminar el panel de control personalizado de tu página de inicio y añadir otro diferente a medida que cambian las prioridades de supervisión.

Haz un seguimiento de lo que realmente importa

Las plantillas de tarjetas están organizadas por tipo de métrica, así puedes centrar un panel de control en un área operativa concreta. Por ejemplo, usa tarjetas de capacidad para vigilar un volumen que está creciendo más rápido de lo esperado, o tarjetas de alerta para hacer un seguimiento de los fallos recurrentes en un clúster con mucha actividad:

Rendimiento
: Latencia, IOPS, rendimiento, utilización y capacidad de rendimiento en toda la flota, los sistemas, las SVM, los volúmenes y los LUN.

Capacidad
: Capacidad utilizada, capacidad libre, porcentaje de capacidad utilizada y capacidad de snapshots en toda la flota, los sistemas, los SVM, los volúmenes, los LUN y los niveles locales.

Salud
: Estado de salud, recuentos de objetos degradados o críticos, discos fallidos, errores de interfaz de red y objetos activos.

Alertas
: Número de alertas críticas, alertas por gravedad, alertas por área de impacto, alertas recientes y tendencias de alertas a lo largo del tiempo.

Para consultar el catálogo completo de tarjetas y métricas predefinidas, consulta "Conoce las tarjetas personalizadas del panel y las métricas en la implementación local de NetApp Console".

Tipos de recursos

Puedes aplicar tarjetas a cualquier nivel de la jerarquía de almacenamiento de ONTAP: flota, clúster, sistema (nodo), SVM, volumen, LUN y nivel local (agregado). Los tipos de recursos disponibles dependen de la plantilla de tarjeta que selecciones.

Planificar vistas del panel de control

Organiza paneles personalizados en función de los objetivos de administración del almacenamiento, como la evaluación del rendimiento de las cargas de trabajo, la planificación de capacidad, la detección de riesgos y la priorización de alertas.

Información relacionada

- "Empieza con los paneles de control en la implementación local de NetApp Console"
- "Ver las métricas de la página de inicio en NetApp Console en una implementación local"
- "Conoce las tarjetas personalizadas del panel y las métricas en la implementación local de NetApp Console"

Empieza con los paneles de control en la implementación local de NetApp Console

En una implementación local de NetApp Console, sigue este flujo de trabajo para monitorear desde vistas generales hasta vistas específicas: revisa el panel de inicio,

revisa los paneles predefinidos, crea paneles personalizados y mantén los paneles actualizados.

Roles de acceso necesarios

Todos los roles. Los paneles de control solo muestran los recursos que estás autorizado a ver. Si no ves un recurso en la lista de recursos disponibles, no tienes permiso para verlo.

Consulta el estado de salud inicial en la página de inicio

Utiliza el panel de control de la página de inicio para consultar la capacidad a nivel de organización, las alertas, el rendimiento y el estado de la protección de datos.

- "Ver las métricas de la página de inicio en NetApp Console en una implementación local"
- "Conoce la supervisión del almacenamiento en la implementación local de NetApp Console"

Consulta otros paneles predefinidos

Abre **Almacenamiento > Paneles** para revisar los paneles predefinidos y ver vistas adicionales específicas para cada rol.

- "Gestiona los paneles de control en la implementación local de NetApp Console"

Crea paneles personalizados para una supervisión específica

Crea paneles personalizados cuando necesites vistas específicas para determinados recursos, métricas y periodos de tiempo.

- "Crear un panel de control personalizado"
- "Personaliza las tarjetas del panel de control en la implementación local de NetApp Console"

Mantén los paneles de control actualizados

Actualiza los paneles de control a medida que cambian las prioridades editando, duplicando o eliminando los paneles personalizados.

- "Gestiona los paneles de control en la implementación local de NetApp Console"
- "Conoce las tarjetas personalizadas del panel y las métricas en la implementación local de NetApp Console"

Información relacionada

- "Conoce los paneles personalizados en la implementación local de NetApp Console"
- "Ver las métricas de la página de inicio en NetApp Console en una implementación local"

Crea paneles para supervisar los objetivos en la implementación local de NetApp Console

Crea un panel personalizado en la implementación local de NetApp Console, añade tarjetas y guarda una vista de supervisión para las operaciones diarias.

Si solo necesitas una supervisión a nivel de organización que esté lista para usar, empieza con los paneles predefinidos de la página de inicio. Crea un panel personalizado cuando necesites una vista específica para un rol, una selección a nivel de recursos o un diseño de tarjetas a medida.

Directrices para el panel de control de implementación local de NetApp Console

- Solo el usuario que crea el panel de control puede verlo. No puedes compartir los paneles de control con otros usuarios, ni siquiera cuando los añades a la página de inicio de NetApp Console.
- Solo puedes ver los recursos para los que tienes permiso. Si no ves un recurso en la lista de recursos disponibles, no tienes permiso para verlo.
- Antes de empezar, identifica los tipos de métricas y los recursos que quieres que el panel de control supervise. "Conoce las tarjetas personalizadas del panel y las métricas en la implementación local de NetApp Console"

Crea un panel de control para tus objetivos de supervisión

Crea un panel de control cuando necesites un único lugar para supervisar las métricas que importan para tu rol, como el estado de la flota, los puntos críticos de rendimiento y las tendencias de alertas.

Pasos

1. Selecciona **Storage > Dashboards**.
2. Selecciona **Add Dashboard**.

   La implementación local de la consola crea un nuevo panel de control con un nombre predeterminado y sin descripción.

3. Selecciona **Add Card**.
4. Selecciona el **tipo de recurso** de la tarjeta, como flota, sistema o volumen y luego elige los recursos de la lista de recursos disponibles.
5. Selecciona **Siguiente** para continuar y elegir una métrica y un tipo de tarjeta.
6. Elige una métrica para mostrar. Puedes filtrar las métricas disponibles por tipo: el **Tipo de métrica**: **Rendimiento**, **Capacidad**, **Estado** o **Alertas** o buscar una métrica concreta por nombre. Las métricas disponibles dependen del tipo de recurso que seleccionaste.

   "Infórmate sobre las métricas disponibles."

7. Selecciona una tarjeta para incluirla en el panel de control y selecciona **Siguiente**.

   Solo puedes seleccionar una tarjeta a la vez. La vista previa de la tarjeta muestra datos en tiempo real para la métrica y el tipo de recurso seleccionados.

8. Asigna un nombre a tu tarjeta. El nombre debe ser único dentro del panel de control.
9. Revisa la vista previa de la ficha, introduce un nombre y una descripción para la ficha y, a continuación, selecciona **Add**.
10. Repite estos pasos para las tarjetas adicionales.
11. Selecciona el icono del lápiz para editar el nombre y la descripción del panel de control y describir su propósito.
12. Selecciona el menú de acciones situado a la derecha del botón Add card y selecciona **Save dashboard**.

    El panel guardado está disponible en **Almacenamiento > Paneles**.

13. Si lo deseas, puedes añadir este dashboard a tu página de inicio seleccionando **Add to Home page** en el menú de acciones. El dashboard se añade a la página de inicio. Solo tú puedes ver los dashboards personalizados que crees. No se comparte con otras personas.

Información relacionada

- "Ver las métricas de la página de inicio en NetApp Console en una implementación local"
- "Conoce los paneles personalizados en la implementación local de NetApp Console"
- "Personaliza las tarjetas del panel de control en la implementación local de NetApp Console"
- "Gestiona los paneles de control en la implementación local de NetApp Console"

Personaliza tarjetas en la implementación local de NetApp Console

En una implementación local de NetApp Console, personaliza las tarjetas del panel cuando necesites que los operadores se centren en las señales que más importan, como el riesgo de SLA, la presión de capacidad o el ruido de alertas recurrentes. Usa este tema para adaptar las vistas del panel a las decisiones operativas que tu equipo necesita tomar.

Antes de empezar

- Crea o abre un panel en el que quieras colocar las tarjetas.
- Consulta las plantillas y métricas disponibles en "Conoce las tarjetas personalizadas del panel y las métricas en la implementación local de NetApp Console".

Agrega tarjetas mientras perfeccionas un panel de control existente

Utiliza esta opción cuando estés perfeccionando un panel de control ya existente y necesites añadir rápidamente tarjetas que respondan a una pregunta operativa concreta.

Pasos

1. Abre el panel de control al que quieras añadir una tarjeta.
2. Selecciona **Add Card**.
3. Selecciona el **tipo de recurso** de la tarjeta, como flota, sistema o volumen y luego elige los recursos de la lista de recursos disponibles.
4. Selecciona **Siguiente** para continuar y elegir una métrica y un tipo de tarjeta.
5. Elige una métrica para mostrar. Puedes filtrar las métricas disponibles por tipo: el **Tipo de métrica**: **Rendimiento**, **Capacidad**, **Estado** o **Alertas** o buscar una métrica concreta por nombre. Las métricas disponibles dependen del tipo de recurso que seleccionaste.

   "Infórmate sobre las métricas disponibles."

6. Selecciona una tarjeta para incluirla en el panel de control y selecciona **Siguiente**.

   Solo puedes seleccionar una tarjeta a la vez. La vista previa de la tarjeta muestra datos en tiempo real para la métrica y el tipo de recurso seleccionados.

7. Asigna un nombre a tu tarjeta. El nombre debe ser único dentro del panel de control.
8. Revisa la vista previa de la ficha, introduce un nombre y una descripción para la ficha y, a continuación,

selecciona **Add**.

9. Repite estos pasos para las tarjetas adicionales.
10. Guarda el panel de control.

Información relacionada

- "Ver las métricas de la página de inicio en NetApp Console en una implementación local"
- "Conoce los paneles personalizados en la implementación local de NetApp Console"
- "Crear un panel de control personalizado"
- "Gestiona paneles personalizados"
- "Conoce las tarjetas personalizadas del panel y las métricas en la implementación local de NetApp Console"

Referencia de los paneles predefinidos y las tarjetas de panel personalizadas en la implementación local de NetApp Console

En una implementación local de NetApp Console, los paneles predefinidos y las plantillas personalizadas de tarjetas de panel proporcionan cobertura de supervisión para el rendimiento, la capacidad, el estado y las operaciones de alerta de ONTAP.

Cuadros de mando predefinidos

Los siguientes paneles predefinidos están disponibles de serie.

Nombre	Descripción
Volúmenes	Rendimiento de volumen, capacidad, QoS, FabricPool, tasa de crecimiento y métricas de previsión.
Tiempo hasta que se llene	Predicciones de ONTAP sobre el tiempo hasta el llenado completo para clústeres, volúmenes y agregados.
Seguridad	Resumen sobre el cumplimiento de las normas de seguridad, el cifrado, la protección autónoma contra ransomware y la autenticación.
SVM	Supervisión del rendimiento, la capacidad, el volumen, el LIF, el protocolo (CIFS, FCP, iSCSI, NFS, NVMe/FC), la QoS y el mapa de calor de latencia de ONTAP SVM.
Potencia	Supervisión del consumo energético, la temperatura y la velocidad de los ventiladores del clúster ONTAP para nodos, estantes y agregados.
Nodos	Supervisión del rendimiento de los nodos ONTAP, la CPU, la red y el backend.
Red	Métricas de rendimiento de la red, entre las que se incluyen Ethernet, FibreChannel, NVMe/FC, grupos de agregación de enlaces y rutas.
LUN	Supervisión del rendimiento, la capacidad y la eficiencia de los LUN de ONTAP.
Salud	Supervisión del estado del clúster ONTAP, incluyendo errores, advertencias, alertas EMS, problemas de HA, estado de nodos, discos y bandejas, volúmenes, licencias y puertos de red.

Nombre	Descripción
Agregados	Supervisión de la capacidad de los agregados de ONTAP, los índices de eficiencia y la tasa de crecimiento.

Ventanas temporales y agregación a nivel del panel de control

Los intervalos de tiempo disponibles son 30 minutos, 1 hora, 24 horas, 48 horas, 7 días y 30 días. Las opciones de agregación varían según la plantilla e incluyen vistas como el resumen de toda la flota o resultados del tipo top-N. El intervalo de tiempo y la agregación se configuran a nivel del panel de control y se aplican a todas las tarjetas del panel de control.

Plantillas de tarjetas y métricas del panel de control

Las tarjetas son los elementos básicos de los paneles personalizados. Cada tarjeta utiliza una plantilla predefinida con una métrica y un tipo de gráfico, luego asocia esa vista a objetos ONTAP específicos y a objetivos de supervisión.

Las plantillas de tarjetas están predefinidas y no las crea el usuario.

Índice de métricas de operaciones de almacenamiento (de un vistazo)

Los tipos de métricas se ajustan a los resultados habituales de la administración del almacenamiento, incluyendo cuellos de botella de rendimiento, presión sobre la capacidad, riesgos para la salud y volumen de alertas.

Tipo de métrica	Métricas compatibles	Caso de uso de administrador de almacenamiento	Plantillas detalladas
Rendimiento	Latencia media, latencia máxima, IOPS, rendimiento (MB/s), utilización, capacidad de rendimiento	Identifica los cuellos de botella, la presión constante y el margen de rendimiento	Ir a las plantillas
Capacidad	Capacidad utilizada, capacidad libre, capacidad utilizada (%), capacidad utilizada en instantáneas	Haz un seguimiento del crecimiento, identifica las áreas con baja capacidad libre y supervisa el impacto de las instantáneas	Ir a las plantillas
Salud	Estado de salud, objetos deteriorados o en estado crítico, discos averiados, errores en la interfaz de red, objetos calientes (por latencia)	Detecta regresiones en el estado de salud y prioriza el triaje operativo	Ir a las plantillas
Alertas	Alertas (críticas), alertas por gravedad, alertas por área de impacto, alertas recientes, tendencia de alertas	Supervisa los incidentes activos y la tendencia del volumen de alertas a lo largo del tiempo	Ir a las plantillas

Jerarquía de objetos compatible de ONTAP (tipos de recursos)

Los datos de tarjetas pueden representarse en varios niveles de objetos de ONTAP, desde la visibilidad a nivel de flota hasta la resolución de problemas a nivel de objeto.

Los ajustes de **Tipo de recurso** se corresponden con uno o varios de los siguientes niveles de recurso:

- Flota
- Clúster
- Sistema (nodo)
- SVM
- Volumen
- LUN
- Nivel local (agregado)

Los niveles de recursos disponibles dependen de la plantilla y la métrica que selecciones.

Tipos de gráficos para el análisis operativo

El tipo de gráfico influye en la rapidez con la que puedes interpretar las tendencias, comparaciones, distribuciones y los valores en un momento específico.

Tipo de gráfico	Ideal para
Gráfico de líneas	Tendencias de series temporales, como la latencia, las IOPS, el rendimiento, la utilización y las tendencias de alertas a lo largo del tiempo.
Gráfico de barras	Comparación y distribución por categorías, como las alertas según su gravedad o área de impacto.
Gráfico circular o de rosquilla	Distribución proporcional, como el porcentaje de capacidad utilizada.
Tabla	Datos detallados, presentados en varias columnas, como la capacidad utilizada, el estado de funcionamiento y las alertas recientes.
Número único (stat)	Un único valor clave de un solo vistazo, como el número de alertas críticas o discos fallidos.

Plantillas de rendimiento para la clasificación de cargas de trabajo

Las plantillas de rendimiento se centran en las señales de latencia, rendimiento y utilización que indican presión de la carga de trabajo.

Plantilla	Tipo de gráfico	Descripción
Latencia media	Línea	Latencia media en los objetivos seleccionados durante el intervalo de tiempo elegido.
Latencia máxima	Línea	Latencia máxima observada en los objetivos seleccionados durante el intervalo de tiempo elegido.
IOPS	Línea	Suma de las operaciones de E/S por segundo en los destinos seleccionados.
Rendimiento (MB/s)	Línea	Suma del caudal de datos en los objetivos seleccionados.
Utilización	Línea	Utilización media de CPU o disco en los objetivos seleccionados.
Capacidad de rendimiento	Tabla	Análisis del margen de capacidad que compara la utilización actual con el punto óptimo.

Plantillas de capacidad para el crecimiento y el margen de maniobra

Las plantillas de capacidad se centran en el espacio consumido y disponible para facilitar la planificación del crecimiento y la detección de riesgos.

Plantilla	Tipo de gráfico	Descripción
Capacidad utilizada	Tabla	Suma de la capacidad utilizada en los objetivos seleccionados.
Capacidad libre	Tabla	Suma de la capacidad libre o disponible en los destinos seleccionados.
Capacidad utilizada (%)	Gráfico circular o de rosquilla	Proporción media de usado a total en los objetivos seleccionados.
Capacidad utilizada de snapshot	Tabla	Suma del espacio ocupado por las instantáneas en los destinos seleccionados.

Plantillas de estado para la detección de riesgos

Las plantillas de estado se centran en el estado de los objetos y en los indicadores de fallo para facilitar la clasificación operativa.

Plantilla	Tipo de gráfico	Descripción
Estado de salud	Tabla	Estado de salud más reciente de cada objeto de destino seleccionado.
Objetos degradados o en estado crítico	Un solo número	Cantidad de objetos cuyo estado de salud no es OK.
Discos averiados	Un solo número	Suma de discos fallidos en los sistemas seleccionados.
Errores de interfaz de red	Gráfico circular o de rosquilla	Suma de los contadores de errores de la interfaz de red en los objetivos seleccionados.
Objetos calientes (por latencia)	Tabla	Recursos ordenados por latencia máxima, en orden descendente.

Plantillas de alertas para la priorización de incidencias

Las plantillas de alertas se centran en el volumen de incidencias, la gravedad y el área de impacto para apoyar la supervisión y la priorización.

Plantilla	Tipo de gráfico	Descripción
Alertas (críticas)	Un solo número	Recuento de alertas de gravedad crítica dentro del intervalo de tiempo.
Alertas por gravedad	Barra	Alertas agrupadas por nivel de gravedad.
Alertas por área de impacto	Barra	Alertas agrupadas por área de impacto, como capacidad, rendimiento o seguridad.
Alertas recientes	Tabla	Las alertas más recientes, ordenadas por hora en orden descendente.

Plantilla	Tipo de gráfico	Descripción
Tendencia de alertas	Línea	Número de alertas por intervalo de tiempo durante la ventana de tiempo seleccionada.

Información relacionada

- "Ver las métricas de la página de inicio en NetApp Console en una implementación local"
- "Conoce los paneles personalizados en la implementación local de NetApp Console"
- "Crear un panel de control personalizado"
- "Personaliza las tarjetas del panel de control en la implementación local de NetApp Console"
- "Gestiona paneles personalizados"

Gestiona paneles personalizados

Gestiona los paneles de control en la implementación local de NetApp Console

Gestiona los paneles personalizados en NetApp Console implementación local para mantener las vistas alineadas con las operaciones. Puedes editar, duplicar y eliminar paneles a medida que cambian los equipos, las flotas y las prioridades.

Esta tarea solo se aplica a los paneles personalizados de **Almacenamiento > Paneles**. Los paneles predefinidos de la página de inicio no se pueden editar de la misma manera.

Ver paneles de control

Consulta los paneles personalizados y predefinidos para encontrar el panel que quieras abrir, editar, duplicar o eliminar.

Puedes duplicar un panel predefinido para crear una versión personalizada que puedas editar.

Pasos

1. Selecciona **Storage > Dashboards**.
2. Revisa la tabla del dashboard para encontrar el dashboard que deseas abrir.
3. Selecciona el nombre del panel de control para abrirlo y ver sus métricas.
4. Si es necesario, utiliza las acciones disponibles para editar, duplicar o eliminar los paneles personalizados.

Actualiza un panel de control a medida que cambian las prioridades

Modifica un panel de control cuando cambien tus prioridades operativas y necesites ajustar qué tarjetas y métricas son visibles.

Pasos

1. Selecciona **Storage > Dashboards**.
2. Abre el panel que quieras editar.
3. Modifica una ficha existente en el panel de control seleccionando Editar en el menú de acciones de la ficha.
4. Agrega una nueva tarjeta al panel seleccionando **Add Card**.

"Personaliza tarjetas en la implementación local de NetApp Console".

5. Selecciona **Guardar cambios** para guardar el panel de control.
   - También puedes optar por guardar los cambios como un nuevo panel de control seleccionando **Guardar como nuevo panel de control** en el menú de acciones. Esta opción es útil cuando quieres conservar el panel de control original para otros equipos o flotas mientras creas una nueva versión para tus necesidades actuales de supervisión.
   - También puedes optar por descartar tus cambios seleccionando **Descartar cambios** en el menú de acciones. Esta opción es útil cuando quieres volver a la última versión guardada del panel.

Reutiliza un panel de control personalizado para otro recurso o flota

Duplica un panel de control cuando quieras reutilizar un diseño que ya ha demostrado su eficacia para otro equipo, flota o escenario de supervisión sin tener que volver a crearlo desde cero.

Puedes duplicar un panel predefinido para crear una versión personalizada que puedas editar.

Pasos

1. Selecciona **Storage > Dashboards**.
2. Para el panel que deseas duplicar, selecciona **Duplicar** en el menú de acciones.

   La implementación local desde la consola crea una copia que incluye todas las tarjetas del panel de control original.

3. Introduce un nombre y una descripción para el panel duplicado.
4. Selecciona el panel duplicado que acabas de crear. Modifica las métricas, los recursos y los tipos de tarjetas para adaptarlos a tu nuevo escenario de supervisión.

   "Personaliza tarjetas en la implementación local de NetApp Console".

Elimina los paneles que ya no utilices

Elimina un panel de control cuando ya no sea compatible con las operaciones actuales y quieras que tu lista de paneles se centre en los casos de uso activos.

Pasos

1. Selecciona **Storage > Dashboards**.
2. Para el panel que quieras eliminar, selecciona **Eliminar**.
3. Confirma la eliminación.

Información relacionada

- "Ver las métricas de la página de inicio en NetApp Console en una implementación local"
- "Empieza con los paneles de control en la implementación local de NetApp Console"
- "Conoce los paneles personalizados en la implementación local de NetApp Console"
- "Crear un panel de control personalizado"
- "Personaliza las tarjetas del panel de control en la implementación local de NetApp Console"

Supervisa flotas utilizando el inventario en la implementación local de NetApp Console

En una implementación local de NetApp Console, utiliza el inventario para supervisar el estado de la flota e investigar los recursos de almacenamiento en todo tu entorno. El inventario ofrece vistas de capacidad, seguridad y rendimiento que te ayudan a identificar problemas, comprender el uso de la capacidad y hacer un seguimiento de los sistemas de almacenamiento gestionados.

«Inventario» es, ante todo, un espacio de trabajo informativo y de diagnóstico. Desde «Inventario», puedes revisar los sistemas, volúmenes y otros objetos de almacenamiento de todas tus flotas y realizar acciones habituales como el aprovisionamiento de recursos de almacenamiento. Para operaciones avanzadas de gestión del almacenamiento, la implementación local de NetApp Console te redirige a System Manager.

Acceder al inventario

Puedes acceder a **Inventario** desde varias áreas de la implementación local de Console, incluyendo:

- La página de inicio
- Páginas de información general de la flota
- Fichas de estado de la flota y vistas de inventario relacionadas

Dependiendo de dónde accedas a **Inventory**, el ámbito que se muestre puede ser a nivel de organización o a nivel de flota.

Vistas de inventario

Inventario ofrece varias vistas que te ayudan a analizar diferentes aspectos de tu entorno de almacenamiento.

Capacidad
: Consulta el uso de la capacidad e identifica los sistemas, volúmenes y otros objetos de almacenamiento que consumen recursos de almacenamiento.

Seguridad
: Revisa la información relacionada con la seguridad y el estado de cumplimiento en los recursos de almacenamiento gestionados.

Rendimiento
: Analiza los indicadores relacionados con el rendimiento e identifica los recursos que puedan requerir un análisis más detallado.

La información que se muestra varía en función de la vista seleccionada y del tipo de objeto.

Investiga los recursos de almacenamiento

Utiliza **Inventario** para:

- Supervisa el estado de la flota
- Revisa el uso de la capacidad de almacenamiento
- Supervisa los sistemas de almacenamiento gestionados

- Identifica los volúmenes y otros objetos que consumen capacidad
- Investiga posibles problemas de seguridad o rendimiento
- Localiza los recursos que requieren atención administrativa

Inventario te ayuda a pasar de una visión a grandes rasgos de tu entorno a un análisis más detallado de recursos de almacenamiento específicos.

Proporciona recursos de almacenamiento

El inventario incluye flujos de trabajo que te permiten aprovisionar recursos de almacenamiento, como volúmenes y LUN.

Al aprovisionar recursos, seleccionas un sistema de almacenamiento gestionado ya existente y proporcionas los parámetros de configuración necesarios para la carga de trabajo.

Inventario y alertas

Se generan alertas para objetos de almacenamiento y condiciones específicas dentro de tu entorno.

Al seleccionar una alerta, la implementación local de Console podría redirigirte a System Manager para realizar investigaciones adicionales o llevar a cabo acciones de gestión. **Inventory** complementa las alertas al ofrecer una visión más amplia del estado general de tu entorno de almacenamiento y de los recursos gestionados.

Tareas de gestión avanzadas

Inventario te ayuda a identificar los recursos que requieren una intervención, pero algunas operaciones avanzadas de gestión del almacenamiento se realizan en System Manager.

Por ejemplo:

- Gestión avanzada de la carga de trabajo
- Tareas de reubicación y optimización de recursos
- Actividades detalladas de administración del sistema

Utiliza **Inventario** para identificar e investigar problemas y luego usa System Manager cuando necesites capacidades de administración más avanzadas.

Corregir alertas

Conoce las alertas en la implementación local de NetApp Console

La implementación local de NetApp Console genera alertas que identifican problemas de estado en tus clústeres ONTAP locales y en las operaciones de NetApp Backup and Recovery.

La implementación local de la consola agrupa las alertas de los clústeres ONTAP y las operaciones de Backup and Recovery en una única vista. La página de alertas incluye un panel, una lista de alertas y una vista de sistemas, así puedes revisar las alertas de toda la organización o limitarlas a una flota o sistema específico. Cada alerta identifica el sistema afectado, su gravedad y su área de impacto.

Utiliza las alertas en la implementación local de Console para:

- Detecta problemas de capacidad, conectividad, protección de datos, rendimiento y seguridad.
- Prioriza las alertas según su gravedad y área de impacto.
- Abre una alerta en System Manager o Workload Analyzer y luego ejecuta una acción de Fix-It guiada o automatizada cuando la página te ofrezca una.
- Envía notificaciones por correo electrónico a los usuarios con roles de acceso específicos o envía datos de alertas a un sistema externo a través de un webhook.
- Exporta la lista de alertas a un archivo CSV para analizarla sin conexión.

Gravedad de las alertas y áreas de impacto

Cada alerta incluye un nivel de gravedad y un ámbito de impacto:

- **Gravedad** indica el nivel de urgencia, de mayor a menor: Crítico, Importante, Menor, Advertencia e Información.
- **Área de impacto** identifica el ámbito afectado: capacidad, conectividad, protección de datos, rendimiento y seguridad.

Fuentes y alcance de las alertas

- **Las alertas de ONTAP** proceden del Sistema de Gestión de Eventos (EMS) de ONTAP en los clústeres locales que ha detectado la implementación local de Console. "Obtén más información sobre el ONTAP EMS y las alertas disponibles."
- **Las alertas de NetApp Backup and Recovery** se originan a partir de acciones de Backup and Recovery. "Obtén más información sobre las alertas de NetApp Backup and Recovery."
- Tus permisos determinan qué flotas puedes ver. Limita la vista a toda la organización, a una flota específica o a un sistema concreto. La pestaña **Estado de los sistemas** muestra el estado de cada sistema y la pestaña **Alertas** muestra la lista actual de alertas para el ámbito seleccionado.
- La exportación a CSV refleja el alcance actual, el texto de búsqueda y los filtros.

Reglas de notificación de alertas

Crea reglas de notificación para determinar qué alertas generan notificaciones y quién las recibe. Una regla de notificación tiene las siguientes características:

- Coincide con las alertas del servicio (como ONTAP management o NetApp Backup and Recovery), la gravedad, el área de impacto y el sistema de destino.
- En el caso de la entrega por correo electrónico, envía notificaciones a los usuarios con los roles de acceso especificados. En el caso de la entrega mediante webhook, envía los datos de las alertas al punto final configurado; el acceso a dichos datos lo controla la aplicación receptora, no la implementación local de Console.
- Se aplica a sistemas concretos, no a flotas.
- Se puede silenciar durante una ventana de mantenimiento planificada para suprimir las alertas esperadas.

La implementación local de la Console incluye una regla de notificación predeterminada que está activa inmediatamente después de la instalación. La regla predeterminada supervisa todos los servicios y sistemas en busca de alertas de gravedad crítica y envía notificaciones solo al Centro de notificaciones de la Console; no se configura el envío por correo electrónico ni mediante webhook hasta que tú lo configures. Puedes ver y ajustar esta regla, y crear reglas personalizadas que se adapten a tu entorno.

Las alertas de nivel Info se muestran en la página Alertas, pero no se envían mediante notificaciones a menos

que crees explícitamente una regla que incluya el nivel de gravedad Info.

Información relacionada

- "Supervisa e investiga las alertas"
- "Crear y gestionar reglas de notificación de alertas"
- "Conoce las alertas de ONTAP en la implementación local de NetApp Console"

Supervisa e investiga alertas en la implementación local de NetApp Console

Supervisa e investiga las alertas en la implementación local de NetApp Console para mantener tu almacenamiento en buen estado y minimizar las interrupciones.

Consulta las alertas activas en toda tu organización o en una flota concreta, priorízalas según su gravedad y el área de impacto, e investiga las causas fundamentales para que puedas resolver los problemas antes de que se agraven. Cuando una alerta incluye una acción recomendada o la opción Fix It, puedes pasar directamente de la investigación a la corrección.

Rol de acceso requerido

Todos los roles excepto Federation admin y Federation viewer. Los usuarios con el rol Federation admin o Federation viewer no pueden ver las alertas. "Conoce los roles de acceso".

En el caso de las alertas de ONTAP, puedes acceder a herramientas como System Manager y Workload Analyzer directamente desde la página de Alertas para investigar y resolver problemas.

Para la elaboración de informes externos, puedes exportar la lista de alertas a un archivo CSV para analizarla sin conexión.

> También puedes configurar reglas de notificación para recibir alertas por correo electrónico o webhook. "Descubre cómo configurar las notificaciones de alerta".

Alertas disponibles

NetApp Console la implementación local admite alertas para ONTAP y NetApp Backup and Recovery.

- "Conoce las alertas de ONTAP en la implementación local de NetApp Console"
- "Obtén más información sobre las alertas de NetApp Backup and Recovery."

Ver el panel de alertas

Utiliza el panel de alertas para obtener una visión general rápida de la actividad actual de alertas en el ámbito que seleccionaste. El panel resume las alertas activas por gravedad y área de impacto, e incluye un gráfico que muestra la distribución de las alertas en las últimas 24 horas para que puedas detectar tendencias rápidamente.

Puedes filtrar el panel de control para centrarte en las alertas críticas o en las alertas de un área de impacto específica.

Pasos

1. Selecciona **Salud > Alertas > Resumen**.
2. En el selector de alcance, elige una de las siguientes opciones:
   - **Todas** (por defecto) para ver las alertas de todas las flotas a las que tienes acceso

- Una flota concreta para ver solo las alertas de esa flota

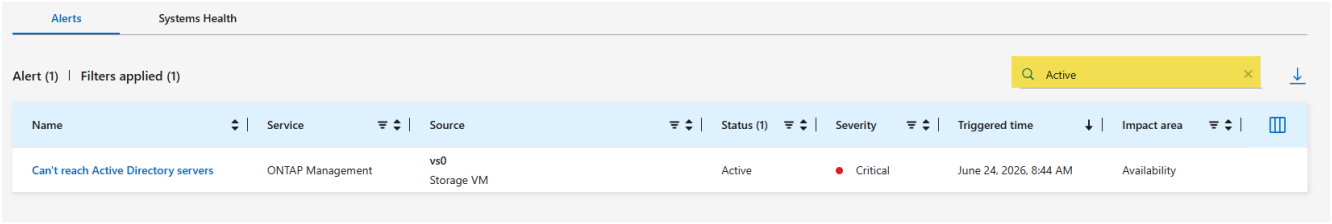
3. Filtra el panel de control según las alertas que necesites ver, entre ellas:
   - Gravedad (crítica, advertencia o informativa)
   - Alertas críticas agrupadas por área de impacto
   - Área afectada (seguridad, protección, disponibilidad, rendimiento, capacidad o configuración)

Ver todas las alertas

Utiliza la pestaña «Alertas» para ver la lista completa de alertas activas correspondientes al ámbito que hayas seleccionado. La lista se actualiza para reflejar el ámbito actual de la organización o la flota, y puedes buscar en la lista alertas específicas por nombre o descripción.

Pasos

1. Selecciona **Salud > Alertas > Resumen**.
2. En el selector de alcance, elige una de las siguientes opciones:
   - **Todas** (por defecto) para ver las alertas de todas las flotas a las que tienes acceso
   - Una flota concreta para ver solo las alertas de esa flota
3. Selecciona la pestaña **Alertas** para ver la lista completa de alertas activas para el ámbito seleccionado.
4. Opcionalmente, busca en la lista una alerta específica por nombre o descripción.



Ver alertas por sistema

Puedes consultar las alertas de un sistema concreto dentro de una flota o tu organización.

Pasos

1. Selecciona **Salud > Alertas > Resumen**.
2. En el selector de alcance, elige una de las siguientes opciones:
   - **Todas** (por defecto) para ver las alertas de todas las flotas a las que tienes acceso
   - Una flota concreta para ver solo las alertas de esa flota
3. Selecciona la pestaña **Estado de los sistemas** para ver un resumen de las alertas relacionadas con los sistemas incluidos en el ámbito que has seleccionado.
4. Selecciona **Ver alertas** en la fila del sistema correspondiente para ver la lista completa de alertas activas asociadas a ese sistema.

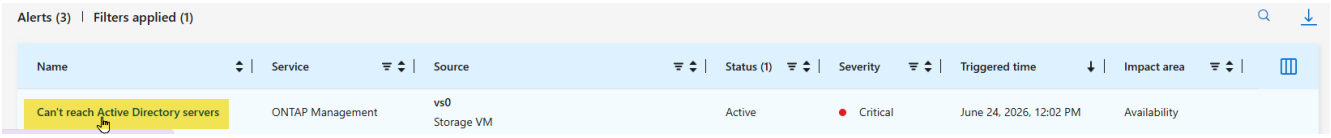
Investigar una alerta

Puedes investigar una alerta para ver qué la activó y quién recibió la notificación.

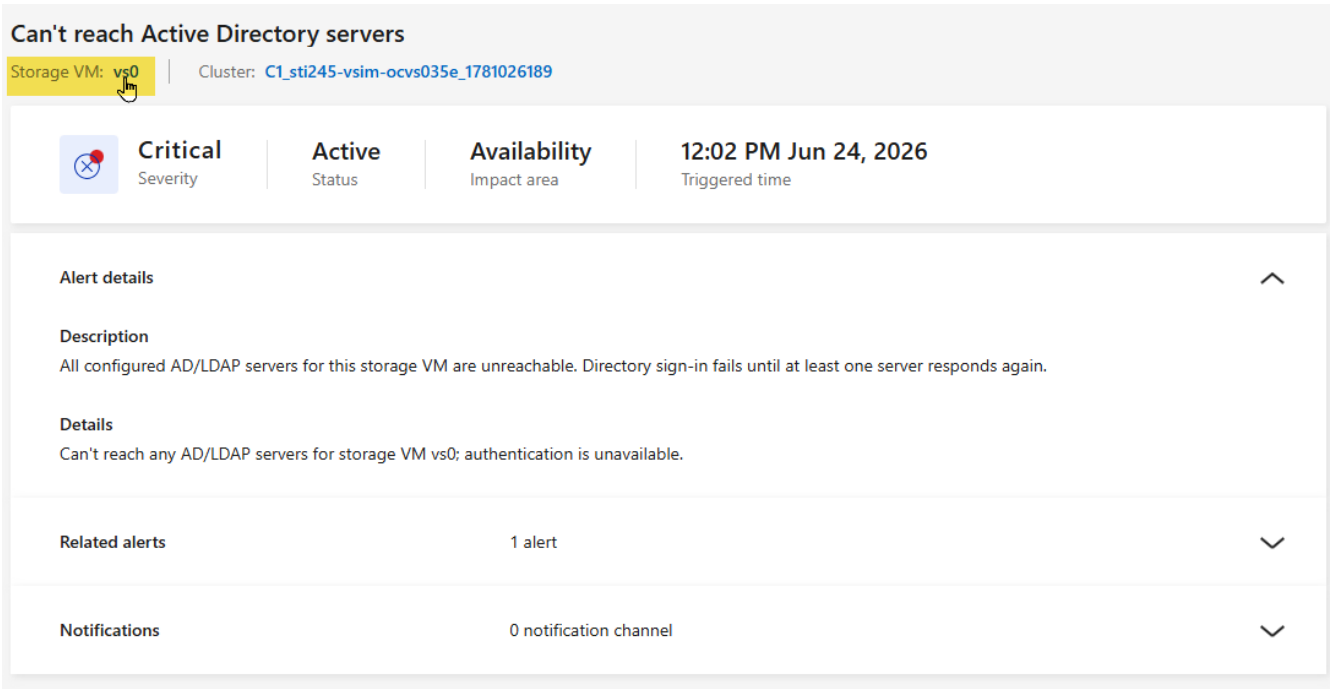
Al investigar una alerta de ONTAP, también puedes acceder directamente a la interfaz de System Manager del sistema que generó la alerta para ver detalles adicionales y tomar medidas.

Pasos

1. Selecciona **Salud > Alertas > Resumen**.
2. En el selector de alcance, elige una de las siguientes opciones:
   - **Todas** (por defecto) para ver las alertas de todas las flotas a las que tienes acceso
   - Una flota concreta para ver solo las alertas de esa flota
3. En cualquiera de las dos pestañas, selecciona el nombre de la alerta que quieras analizar para ver sus detalles.



4. Si procede, selecciona el nombre de la máquina virtual o del clúster para abrir la interfaz de System Manager para el sistema que generó la alerta.



Resolver una alerta

Cuando una alerta incluya una acción recomendada o la opción Fix It, utilízala para pasar de la investigación a la corrección sin salir de los detalles de la alerta.

Pasos

1. Selecciona **Salud > Alertas > Resumen**.
2. En el selector de alcance, elige una de las siguientes opciones:
   - **Todas** (por defecto) para ver las alertas de todas las flotas a las que tienes acceso
   - Una flota concreta para ver solo las alertas de esa flota
3. Selecciona la alerta que quieras solucionar.
4. Revisa los detalles de la alerta y, a continuación, selecciona la acción recomendada o la opción

Solucionar si está disponible.

5. Sigue los pasos indicados para aplicar la solución y luego vuelve a los detalles de la alerta para confirmar el estado de la alerta.

Si la acción resuelve el problema, la alerta ya no aparece como activa para ese ámbito. Si la alerta sigue activa, revisa de nuevo los detalles de la alerta y continúa la investigación.

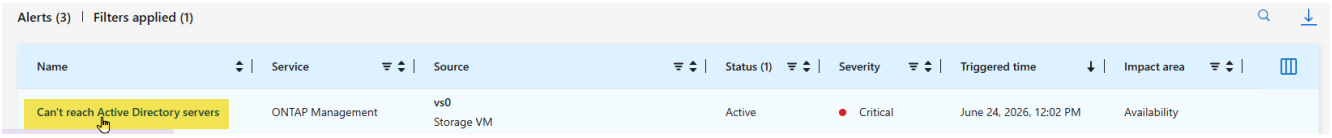
Analizar una alerta

Puedes analizar una alerta de ONTAP en Workload Analyzer para comprender qué la activó.

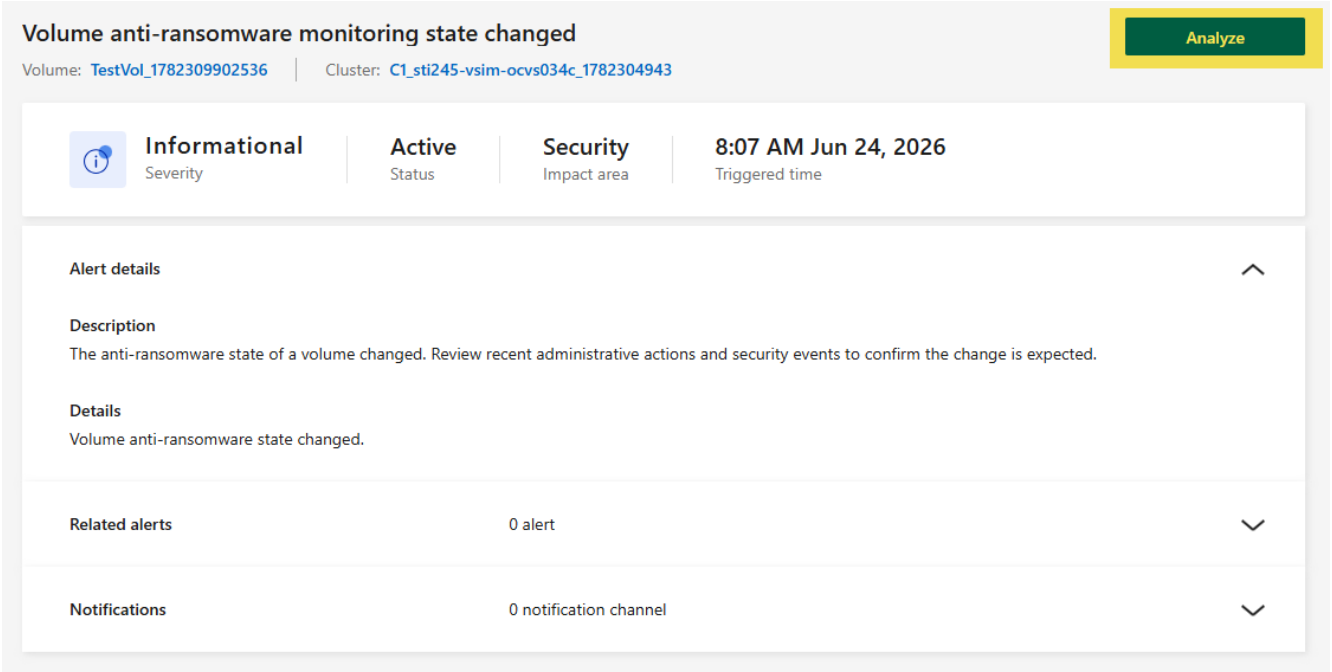
Al investigar una alerta de ONTAP, también puedes acceder directamente a la interfaz de System Manager del sistema que generó la alerta para ver detalles adicionales y tomar medidas.

Pasos

1. Selecciona **Salud > Alertas > Resumen**.
2. En el selector de alcance, elige una de las siguientes opciones:
   - **Todas** (por defecto) para ver las alertas de todas las flotas a las que tienes acceso
   - Una flota concreta para ver solo las alertas de esa flota
3. Selecciona la pestaña **Estado de los sistemas** para ver la lista completa de alertas activas para el ámbito seleccionado.
4. En cualquiera de las dos pestañas, selecciona el nombre de la alerta que quieras analizar para ver sus detalles.



5. Si procede, selecciona **Analizar** para abrir la interfaz del Workload Analyzer del sistema que generó la alerta.



6. Introduce el intervalo de tiempo que abarca el periodo en el que se activó la alerta y, a continuación, selecciona **Analizar** para ver los resultados del análisis. "Conoce Workload Analyzer."

Exportar alertas a CSV

Exporta la lista de alertas en la implementación local de la NetApp Console a un archivo CSV para análisis o informes sin conexión. La exportación refleja el ámbito actual (organización o flota), el texto de búsqueda y los filtros.

Pasos

1. Selecciona **Salud > Alertas** y luego selecciona la pestaña **Alertas**.
2. Establece el ámbito (organización o flota) y aplica cualquier filtro o texto de búsqueda que quieras incluir en la exportación.
3. Selecciona el icono de descarga para exportar la lista de alertas a un archivo CSV.

Configura reglas de notificación para alertas en la implementación local de NetApp Console

Configura las reglas de notificación en la implementación local de NetApp Console para controlar qué alertas generan notificaciones, quién las recibe y cómo se entregan.

Roles de acceso necesarios

Superadministrador, administrador de la organización, administrador de almacenamiento, analista de soporte de operaciones o cualquiera de los roles de administrador de NetApp Backup and Recovery. "Conoce los roles de acceso".

Utiliza las reglas de notificación para dirigir las alertas adecuadas a las personas adecuadas a través de los canales que mejor se adapten a tu entorno, mientras reduces el ruido de las alertas que no son relevantes para ti. Las reglas de notificación complementan la página de Alertas: investigas o resuelves la alerta en el flujo de trabajo de Alertas y luego usas las reglas para controlar cómo se entregarán alertas similares en el futuro.

Una regla de notificación filtra las alertas en función de las condiciones que definas, como el servicio, la gravedad y el área de impacto, y luego envía una notificación a través de los canales que selecciones. La implementación local de NetApp Console incluye reglas de notificación predeterminadas que puedes consultar y ajustar, y puedes crear tus propias reglas personalizadas. También puedes silenciar reglas para suprimir temporalmente las notificaciones durante eventos planificados como ventanas de mantenimiento.

- "Obtén más información sobre el ONTAP EMS y las alertas disponibles."

Antes de empezar

- Para enviar notificaciones por correo electrónico, el administrador de tu organización debe configurar un servidor de correo electrónico en la implementación local de la Console. Para enviar notificaciones a un sistema externo, el administrador de tu organización debe configurar un webhook. Para conocer los pasos, consulta "Configura la entrega de notificaciones".
- El Centro de notificaciones de la implementación local de la Console muestra las notificaciones de forma predeterminada, por lo que no es necesario realizar ninguna configuración adicional para las notificaciones dentro de la Console.

Ver reglas de notificación

La página de reglas de notificación es el lugar central para revisar y gestionar todas las reglas que se aplican a tu organización. Cada regla muestra sus atributos clave para que puedas evaluar y ajustar rápidamente el

comportamiento de las alertas.

Pasos

1. En el menú de navegación de la izquierda, selecciona **Salud > Alertas**.
2. Selecciona **Configuración de notificaciones**.
3. Revisa las reglas de la lista. Cada regla muestra su estado de activación, nombre, los servicios y los niveles de gravedad que supervisa, los roles autorizados para recibir notificaciones, los canales de envío habilitados, cuándo se modificó por última vez y cualquier periodo de silenciamiento programado.
4. Para encontrar una regla concreta, utiliza los controles de filtro y búsqueda para filtrar por estado activo, servicio, gravedad, rol, canal o estado de silenciamiento.

Crear una regla de notificación

Crea una regla de notificación para definir las condiciones que activan una notificación y cómo se entrega esa notificación.

> No puedes configurar reglas de notificación para flotas. Solo puedes configurarlas para sistemas específicos. En entornos grandes con muchos sistemas, considera crear reglas más amplias según la gravedad en lugar de duplicar reglas por sistema; por ejemplo, una regla crítica que abarque todos los sistemas actúa como una regla general, con reglas adicionales específicas para los sistemas que necesiten un enrutamiento o destinatarios diferentes.

Ejemplo de regla de notificación para alertas críticas en todos los sistemas

Supongamos que quieres asegurarte de que ninguna alerta crítica pase desapercibida, independientemente del sistema del que proceda. Puedes crear una regla general que redirija todas las alertas críticas al Centro de notificaciones de la consola para los administradores de almacenamiento.

En este ejemplo, creas una regla con los siguientes parámetros:

- **Servicios**: todos
- **Gravedad**: Crítica
- **Rol de IAM**: administrador de almacenamiento
- **Sistema**: (Déjalo en blanco para que se aplique a todos los sistemas)
- **Método de entrega**: Centro de notificaciones de la consola

Con esta regla activada, los administradores de almacenamiento ven una notificación en la Console por cada alerta crítica en todos los sistemas. Esta regla sirve como base que puedes complementar con reglas más específicas.

Ejemplo de una regla de notificación específica para alertas de capacidad de Storage admin

Supongamos que tus administradores de almacenamiento necesitan responder de inmediato a problemas críticos de capacidad en un sistema de producción concreto, pero no quieres que sus bandejas de entrada se vean inundadas de alertas de menor gravedad. Puedes crear una regla específica para que se envíe un correo electrónico a los administradores de almacenamiento solo cuando se active una alerta crítica de capacidad en ese sistema.

En este ejemplo, creas una regla con los siguientes parámetros:

- **Servicios**: gestión de ONTAP
- **Gravedad**: Crítica

- **Ámbito de impacto**: Capacidad
- **Rol de IAM**: administrador de almacenamiento
- **Sistema**: <system_name>
- **Método de entrega**: Correo electrónico

Con esta regla activada, Console envía un correo electrónico a todos los administradores de almacenamiento del sistema especificado cuando se produce una alerta de capacidad crítica. Las alertas de menor gravedad, como las de advertencia o las informativas, no generan ningún correo electrónico, así que el equipo puede centrarse en los problemas que requieren atención urgente.

Pasos

1. En el menú de navegación de la izquierda, selecciona **Salud > Alertas**.
2. Selecciona **Configuración de notificaciones** y, a continuación, selecciona **Agregar regla**.
3. Define las condiciones que la regla debe cumplir:
   - **Nombre de la regla**: introduce un nombre conciso y descriptivo. Este campo es obligatorio.
   - **Descripción de la regla**: opcionalmente, introduce información adicional sobre la finalidad de la regla.
   - **Servicios**: selecciona uno o varios servicios de ONTAP o de la plataforma a los que se aplique la regla.
   - **Roles**: selecciona los roles de acceso que deben tener los usuarios para recibir notificaciones cuando se active la regla.
   - **Niveles de gravedad**: selecciona los niveles de gravedad que supervisa la regla, como «Crítico», «Advertencia», «Error» o «Información».
   - **Área de impacto**: selecciona las áreas operativas que correspondan, como Capacidad o Rendimiento.
   - **Nombre de la alerta**: selecciona los tipos de alerta específicos que activan la regla.
   - **Sistema**: selecciona el contexto del sistema al que se aplica la regla.
4. Selecciona los canales de envío de la notificación:
   - **Correo electrónico**: envía correos electrónicos de alerta a los usuarios que tengan los roles seleccionados. Requiere un servidor de correo electrónico configurado.
   - **Webhook**: envía datos de alertas a un sistema externo. Requiere seleccionar una integración de webhook configurada.
   - **Centro de notificaciones de la consola**: muestra alertas en tiempo real para los usuarios que tienen los roles seleccionados.
5. Si lo deseas, para desactivar las notificaciones de esta regla durante un periodo planificado, como una ventana de mantenimiento, configura una programación de **Silenciar notificaciones** y elige una periodicidad si quieres que el periodo de silencio se repita. Puedes añadir varias ventanas de silencio por regla, lo cual resulta útil para ciclos de mantenimiento recurrentes como la aplicación semanal de parches.
6. Selecciona **Crear**.

Activar o desactivar una regla de notificación

Activa o desactiva reglas de notificación concretas para controlar qué condiciones generan notificaciones. Desactiva las reglas que no sean relevantes para tu entorno a fin de reducir el ruido y activa las reglas para volver a recibir sus notificaciones.

Pasos

1. En el menú de navegación de la izquierda, selecciona **Salud > Alertas**.
2. Selecciona **Configuración de notificaciones**.
3. Busca la regla que quieras modificar.
4. Activa o desactiva el interruptor **Activo** de la regla. El cambio surte efecto de inmediato.

Silenciar una regla de notificación

Silencia una regla de notificación para evitar que se envíen alertas durante un evento programado, como una ventana de mantenimiento, sin desactivar la regla. Las alertas siguen apareciendo en la página Alertas durante el periodo de silencio; solo se suprimen las notificaciones por correo electrónico, webhook y en la consola. Cuando finaliza el periodo de silencio, las notificaciones se reanudan automáticamente.

Puedes añadir varias ventanas de silencio a una misma regla y configurar cada una para que se repita según una programación.

Ejemplos de ventanas silenciadas

- **Ventana de mantenimiento puntual**: Estás realizando una actualización de firmware en un sistema de almacenamiento el sábado por la noche y quieres silenciar las alertas previstas durante esa ventana. Configura una ventana de silencio desde el sábado a las 22:00 hasta el domingo a las 02:00, sin recurrencia. Cuando finalice la ventana, las notificaciones se reanudan automáticamente.
- **Ventana de actualizaciones semanal recurrente**: Tu equipo aplica las actualizaciones a los sistemas todos los domingos, desde la medianoche hasta las 4:00 de la madrugada. Añade una ventana de silencio con periodicidad semanal para que las notificaciones se silencien automáticamente cada semana sin necesidad de intervención manual. Si un segundo sistema tiene su propio horario de aplicación de parches en un momento diferente, añade una segunda ventana de silencio a la misma regla con su propia hora de inicio y periodicidad.

Pasos

1. En el menú de navegación de la izquierda, selecciona **Salud > Alertas**.
2. Selecciona **Reglas de notificación**.
3. En la lista de reglas, busca la regla que quieras silenciar y selecciona el menú de acciones correspondiente a esa regla.
4. Selecciona **Editar**.
5. En la sección **Silenciar notificaciones**, establece la fecha y la hora de inicio y fin para la ventana de silenciamiento.
6. Si lo deseas, selecciona una periodicidad para que la ventana se repita según un calendario.
7. Para añadir más ventanas de silencio, selecciona **Add mute window** y repite los pasos anteriores.
8. Selecciona **Guardar**.

Eliminar una regla de notificación

Elimina una regla de notificación si ya no la necesitas. Al eliminar una regla, esta se borra de forma definitiva, por lo que no puedes recuperarla.

Pasos

1. En el menú de navegación de la izquierda, selecciona **Salud > Alertas**.
2. Selecciona **Configuración de notificaciones**.
3. En la lista de reglas, busca la regla que quieras eliminar y selecciona el menú de acciones

correspondiente a esa regla.

4. Selecciona **Eliminar** en el menú de acciones.

Información relacionada

- "Configura la entrega de notificaciones"
- "Conoce las alertas de la consola"
- "Ver alertas"

Corrige la desviación de la clase de almacenamiento en la implementación local de NetApp Console

En una implementación local de NetApp Console, encuentra alertas relacionadas con desviaciones, analiza los hallazgos de desviaciones y corrige las cargas de trabajo que ya no coinciden con la intención de su clase de almacenamiento.

Roles requeridos

Administrador de almacenamiento

Solo puedes ver y corregir cargas de trabajo en las flotas donde tengas permiso.

Corregir la deriva

Cuando una carga de trabajo ya no coincide con la intención de su clase de almacenamiento, el despliegue local de NetApp Console genera una alerta. Usa la alerta para analizar la desviación y aplicar la corrección recomendada.

Puedes aplicar algunas medidas correctivas directamente desde la alerta. Para otros problemas, actualiza la configuración de la carga de trabajo o asigna una clase de almacenamiento diferente para restablecer el cumplimiento. El flujo de trabajo de corrección muestra el impacto previsto antes de que apliques los cambios.

Pasos

1. Selecciona **Almacenamiento > Clases de almacenamiento**.

   En el apartado **Variaciones por clase de almacenamiento** aparece un resumen de las variaciones en las clases de almacenamiento. La lista completa figura en la tabla.

2. En la columna **Drifts**, selecciona **Ver** para la clase de almacenamiento correspondiente.

   La página **Alertas > Resumen** se abre con los filtros aplicados.

3. Selecciona una alerta para abrir la página de detalles de la alerta.
4. Selecciona **Analyze**.
5. Revisa los resultados en **Workload analyzer**.

   Para los resultados sobre desviaciones en la configuración, compara los ajustes previstos y los reales para determinar qué cambió.

6. Selecciona la acción correctiva recomendada, como **Fix it**.
7. Revisa los cambios propuestos y aplica la remediación.
8. Vuelve a **Almacenamiento > Clases de almacenamiento** y comprueba que la carga de trabajo ya no

aparece como desviada.

Las evaluaciones de cumplimiento pueden tardar varios minutos en reflejar los cambios de configuración recientes. Si la carga de trabajo sigue apareciendo como desviada, vuelve a la página de detalles de la alerta y selecciona **Analizar** para revisar los resultados restantes.

Información relacionada

- "Conoce la desviación de la clase de almacenamiento y el cumplimiento en la implementación local de NetApp Console"
- "Conoce las alertas de almacenamiento"
- "Ver alertas"

Acciones de corrección de alertas en la implementación local de NetApp Console

Utiliza esta referencia para entender las acciones de corrección disponibles en **Fix it** en la implementación local de NetApp Console. Para cada acción, la tabla describe lo que hace la acción y la alerta relacionada. Revisa los detalles de la acción en el cuadro de diálogo de confirmación antes de ejecutarla.

Acciones de remediación

Acción de remediación	Nombre de la alerta	Descripción de la alerta	Área de impacto	Resumen de corrección
Activar el aumento automático del volumen	Volumen completo	El volumen se está quedando sin espacio y está a punto de alcanzar su capacidad máxima.	Capacidad	Aumenta automáticamente el tamaño de un volumen (hasta un límite configurado) para reducir el riesgo de quedarse sin espacio.
Cambiar el tamaño del volumen	Volumen completo	El volumen se está quedando sin espacio y está a punto de alcanzar su capacidad máxima.	Capacidad	Aumenta el tamaño de un volumen para disponer de más espacio de forma inmediata.
Poner el volumen en línea	Volumen sin conexión	El volumen está sin conexión y no está sirviendo datos.	Disponibilidad	Pone en línea un volumen sin conexión para que pueda volver a proporcionar datos.
Poner en línea el agregado	Agregado sin conexión	El agregado no está en línea y los volúmenes alojados en él pueden no estar disponibles.	Disponibilidad	Pone en línea un agregado sin conexión para restablecer el acceso a los volúmenes que aloja.

Acción de remediación	Nombre de la alerta	Descripción de la alerta	Área de impacto	Resumen de corrección
Poner el LUN en línea	LUN fuera de línea	El LUN está fuera de línea y el acceso al host no está disponible.	Disponibilidad	Pone en línea un LUN sin conexión para que los hosts puedan reanudar el acceso y las operaciones de E/S.
Desbloquear volumen	Volumen restringido	El volumen se encuentra en un estado restringido y es posible que no pueda gestionar las operaciones de E/S con normalidad.	Disponibilidad	Devuelve un volumen restringido a un estado en línea para que los clientes puedan volver a acceder a él.
Poner en línea el espacio de nombres NVMe	El espacio de nombres NVMe está sin conexión	El espacio de nombres NVMe está sin conexión y el acceso al host no está disponible.	Disponibilidad	Activa un espacio de nombres NVMe sin conexión para restablecer el acceso del host.
Activar el LIF entre clústeres	LIF entre clústeres inactivo	Un LIF interclúster está inactivo y la comunicación entre clústeres podría verse afectada.	Conectividad	Activa un LIF interclúster para restablecer la conectividad entre clústeres utilizada para la replicación.
Vuelve a habilitar AUSO de MetroCluster	MetroCluster conmutación de sitios automática no planificada desactivada	La conmutación de sitios automática no planificada está desactivada en este clúster.	Disponibilidad	Vuelve a activar la conmutación de sitios automática no planificada (AUSO) para que la protección MetroCluster funcione como se espera.
Configurar la red del Service Processor	El procesador de servicios no está configurado	La red del procesador de servicios (SP) no está configurada.	Facilidad de gestión	Configura los parámetros de red del Service Processor (SP) para habilitar el acceso de gestión fuera de banda.
Asignar discos sin asignar	Se han detectado discos sin asignar	Hay discos sin asignar y es posible que haya capacidad disponible sin utilizar. Asigna los discos a un nodo para que puedan usarse como almacenamiento.	Disponibilidad	Asigna los discos que actualmente no están asignados a un nodo para que puedan usarse como almacenamiento.

Acción de remediación	Nombre de la alerta	Descripción de la alerta	Área de impacto	Resumen de corrección
Recuperación del espacio en el volumen raíz	Espacio libre en el volumen raíz del nodo insuficiente	El espacio disponible en el volumen raíz del nodo es escaso y puede afectar el funcionamiento normal del sistema.	Estado del sistema	Libera espacio en el volumen raíz del nodo eliminando la instantánea más grande o el archivo de volcado de memoria más grande. Las eliminaciones son permanentes.

Investiga problemas de rendimiento

Obtén información sobre Workload Analyzer para el despliegue local de NetApp Console

Usa el Workload Analyzer de despliegue local de NetApp Console para ver el comportamiento de un solo volumen a lo largo del tiempo. Puedes investigar la degradación del rendimiento, las tendencias de capacidad y los problemas de contención de recursos desde el propio volumen, desde una alerta o desde el inventario.

Cómo identifica Workload Analyzer las causas fundamentales

Utiliza el Analizador de carga de trabajo para correlacionar métricas de un único volumen en seis secciones, así puedes identificar rápidamente las causas raíz. Selecciona un volumen y un intervalo de tiempo para ver eventos, rendimiento y capacidad juntos en la misma ventana. Esta vista puede ayudarte a determinar si el almacenamiento es la fuente probable de un problema de la aplicación o si otra capa, como la red, está causando el problema.

El analizador resulta especialmente útil cuando ya sabes qué volumen está afectado. Si lo abres desde una alerta o desde el inventario de volúmenes, Console local deployment abre el analizador con el volumen seleccionado para que puedas centrarte en la ventana de análisis y en los gráficos.

El analizador examina un volumen cada vez, así que utilízalo para investigar un problema concreto en lugar de comparar varios volúmenes.

Revisa la sección sobre capacidad como parte de esta evaluación. Cuando un sistema ONTAP está lleno en más de un 85 %, la elevada utilización puede provocar por sí misma problemas de rendimiento, por lo que una capacidad disponible baja puede explicar la latencia que los gráficos de rendimiento por sí solos no tienen en cuenta.

Una vez identificada la causa raíz, puedes actuar directamente desde el analizador. Cuando hay opciones automatizadas disponibles, la implementación local de Console ofrece recomendaciones de Fix-It con pasos guiados o corrección con un solo clic.

Los gráficos de carga de trabajo de los LUN no ofrecen el mismo nivel de detalle que los de los volúmenes, por lo que verás menos estadísticas al analizar un LUN.

Accede a Workload Analyzer

Puedes abrir el Analizador de carga de trabajo de varias formas:

- En el menú **Salud**, selecciona **Analizador de carga de trabajo**, luego busca y selecciona el volumen que quieres investigar en el campo **Volumen**.
- Desde la página **Almacenamiento > Flotas > Inventario**, ve a un volumen que quieras analizar y selecciona **Analizar** en el menú de acciones.
- En la página **Alertas > Resumen**, selecciona una alerta para el volumen que quieres investigar y luego selecciona **Analizar** en los detalles de la alerta.

También puedes analizar los LUN, pero muestran menos estadísticas que los volúmenes.

Analiza la latencia, el rendimiento y la capacidad de almacenamiento

Utiliza estas seis secciones para investigar un volumen:

Selección de volumen
: Selecciona el volumen y el intervalo de tiempo que deseas analizar para que todos los gráficos y eventos se alineen con la misma carga de trabajo y ventana de análisis.

Cronología del evento
: Consulta los cambios de configuración actuales e históricos, las alertas de advertencia y las alertas críticas para el volumen seleccionado durante la ventana de análisis. Usa esta sección para correlacionar "qué cambió" con los cambios en el rendimiento o el comportamiento de la capacidad.

Análisis de latencia
: Visualiza la latencia del volumen a lo largo del tiempo, ya sea como valor total o desglosada por centro de retardo: red, procesamiento de datos, operaciones de agregado, interconexión de clúster y otros. Si el volumen utiliza una política de QoS, el analizador muestra los límites máximo y mínimo de latencia de la política como líneas de referencia para que puedas ver qué tan cerca está la carga de trabajo de un umbral de limitación. Activa o desactiva la previsión para proyectar si la latencia tiende hacia un umbral de advertencia o crítico.

Análisis del rendimiento
: Visualiza las IOPS y los MB/s a lo largo del tiempo, con un desglose opcional por lectura/escritura/otros. Si el volumen utiliza una política de QoS, el analizador muestra líneas de límite de IOPS y de rendimiento. Activa o desactiva la previsión para proyectar si la demanda está tendiendo hacia los límites de QoS.

Utilización de recursos
: Consulta qué tan ocupados están los nodos y agregados que dan servicio al volumen durante el periodo de análisis. El analizador representa cada recurso como una línea independiente en lugar de agrupar los valores, así puedes identificar si un nodo o agregado específico es una fuente de contención. Activa o desactiva la previsión para ver si algún recurso está tendiendo hacia un umbral de alta utilización.

Análisis de capacidad
: Consulta cómo han variado el espacio físico y el espacio disponible en el volumen a lo largo del tiempo. Pasa el cursor por encima para ver un desglose de la eficiencia de almacenamiento, incluyendo deduplicación, compresión y ahorros por compactación. Activa o desactiva la previsión para proyectar cuándo el volumen alcanzará los umbrales de capacidad de advertencia o críticos. Cambia a la vista de snapshot para ver cómo el espacio de snapshot se compara con la reserva de snapshot configurada.

Previsión de las tendencias de capacidad y rendimiento

Utiliza el botón de activación de la previsión en cada sección de análisis para ampliar el periodo temporal del gráfico más allá del momento actual y proyectar valores futuros basándose en la tendencia observada. Una línea discontinua distingue los valores de previsión de los datos reales. El analizador también muestra un

mensaje de alerta cuando la previsión indica que es probable que se supere un umbral, junto con un tiempo estimado hasta que se produzca dicho rebasamiento.

Información relacionada

"Investiga la alta latencia en un volumen". "Investiga la demanda de alto rendimiento en un volumen". "Investiga el crecimiento de la capacidad en un volumen". "Aprende sobre las métricas de Workload Analyzer en el despliegue local de NetApp Console".

Investiga la alta latencia en un volumen en una implementación local de NetApp Console

Utiliza Workload Analyzer en la implementación local de NetApp Console para encontrar la causa de los tiempos de respuesta lentos de un volumen.

Si abres el analizador desde una alerta o desde el inventario de volúmenes, el volumen ya está seleccionado y puedes centrarte en el intervalo de tiempo y en los desgloses del gráfico.

Cuando el rendimiento de una aplicación se ve afectado, identifica qué parte de la ruta de I/O está provocando la ralentización. La sección de análisis de latencia desglosa el tiempo de respuesta por centro de retardo, así puedes distinguir entre problemas de red, sobrecarga en el procesamiento de datos, contienda agregada y otros factores que contribuyen.

Pasos

1. Abre Workload Analyzer mediante uno de los siguientes métodos:
   - En el menú **Salud**, selecciona **Analizador de carga de trabajo**, luego busca y selecciona el volumen que quieres investigar en el campo **Volumen**.
   - Desde la página **Almacenamiento > Flotas > Inventario**, ve a un volumen que quieras analizar y selecciona **Analizar** en el menú de acciones.
   - En la página **Alertas > Resumen**, selecciona una alerta relacionada con la capacidad para el volumen que quieres investigar y luego selecciona **Analizar** en los detalles de la alerta.
2. Establece el **Intervalo de tiempo** para que abarque el periodo en el que se produjo el problema de rendimiento, luego selecciona **Analizar**.
3. Consulta la sección **Cronología de eventos** para ver los cambios de configuración y las alertas que coinciden con el aumento de la latencia.

   El analizador representa los eventos de cambio de configuración (icono de la llave inglesa) y los eventos de alerta (iconos de advertencia y críticos) a lo largo del mismo eje temporal que el gráfico de latencia, lo que permite ver fácilmente si un cambio precedió al deterioro.

4. En la sección **Latencia**, abre el menú desplegable **Ver** y selecciona **Desglose por centro de retardo**. El gráfico muestra la contribución de cada centro de retardo a la latencia total a lo largo del tiempo. Los centros de retardo incluyen:
   - Latencia de lectura
   - Latencia de escritura
   - Otra latencia
5. Pasa el cursor por encima de un punto del gráfico donde la latencia sea más alta para ver el valor de cada centro de retardo y su porcentaje respecto a la latencia total.

   El centro de retardo más importante suele indicar cuál es el recurso objeto de conflicto. Cuando un recurso compartido no puede satisfacer la demanda, los volúmenes que lo utilizan esperan más tiempo para la I/O. Reduce la carga sobre ese recurso, por ejemplo, trasladando cargas de trabajo o ajustando un límite de

QoS, para reducir la latencia.

6. Identifica el factor que más influye y usa ese valor para determinar los siguientes pasos:
   - Una **latencia de lectura** elevada puede indicar contención de disco. Consulta la sección **Utilización de recursos** para confirmar el porcentaje de ocupación total.
   - Una **latencia de escritura** elevada puede indicar una saturación de la NIC o problemas en la ruta de red fuera del clúster.
   - Una **Otra latencia** alta puede indicar que los ajustes de eficiencia en línea están consumiendo más CPU de lo que la carga de trabajo puede tolerar. Considera ajustar los ajustes de eficiencia o QoS.
   - Una **latencia en la nube** elevada puede indicar que la carga de trabajo accede con frecuencia a datos fríos en el nivel de capacidad. Considera ajustar la política de tiering.
7. Si los centros de retardo no explican la ralentización, consulta la sección **Análisis de capacidad**. Cuando el sistema ONTAP está lleno en más de 85 %, el elevado uso de la capacidad puede provocar problemas de rendimiento, independientemente del desglose por centros de retardo.
8. Si la latencia aumentó inmediatamente después de un evento de cambio, usa los detalles del evento y los gráficos relacionados juntos para validar la causa probable:
   - Para detectar cambios en la calidad del servicio (QoS), compara la línea de latencia con las líneas de límite de QoS y revisa los gráficos de rendimiento para comprobar si la demanda alcanza el límite máximo establecido en la política.
   - En el caso de movimientos de agregados o de volumen, compara el pico de latencia con los valores de utilización del nodo y del agregado que se muestran para el mismo intervalo de tiempo.
   - En el caso de los cambios en la política de clasificación por niveles, revisa la contribución de la latencia de la nube para determinar si el acceso a los datos inactivos aumentó tras el cambio.

Después de que termines

Si el problema se debe a un error de configuración o de ubicación y la implementación local de Console puede solucionarlo, es posible que la alerta del volumen ofrezca una opción Fix-It.

"Aprende sobre las métricas de Workload Analyzer en el despliegue local de NetApp Console".

Investiga el alto rendimiento en un volumen en una implementación local de NetApp Console

Utiliza Workload Analyzer en la implementación local de NetApp Console para analizar la demanda de IOPS y el rendimiento de un volumen a lo largo del tiempo.

Cuando la carga de trabajo de un volumen consume más IOPS o rendimiento de lo esperado, identifica qué está generando esa demanda. La sección de análisis de rendimiento muestra IOPS y MB/s, con un desglose opcional por lectura, escritura y otros, para que puedas identificar qué tipo de I/O está generando una demanda elevada y si esa demanda tiende hacia un límite de QoS.

Si abres el analizador desde una alerta o desde el inventario de volúmenes, el volumen ya está seleccionado y puedes centrarte en el intervalo de tiempo y los gráficos de rendimiento.

Pasos

1. Abre Workload Analyzer mediante uno de los siguientes métodos:
   - En el menú **Salud**, selecciona **Analizador de carga de trabajo**, luego busca y selecciona el volumen que quieres investigar en el campo **Volumen**.
   - Desde la página **Almacenamiento > Flotas > Inventario**, ve a un volumen que quieras analizar y selecciona **Analizar** en el menú de acciones.

- En la página **Alertas > Resumen**, selecciona una alerta para el volumen que quieres investigar y luego selecciona **Analizar** en los detalles de la alerta.

2. Establece el **Intervalo de tiempo** para que abarque el periodo de demanda elevada y luego selecciona **Analizar**.
3. Desplázate hasta la sección **Throughput Analysis**.
4. Abre el menú desplegable **Ver** y selecciona **Desglose (RWO)**.

   Los gráficos se desglosan en componentes de lectura, escritura y otros, tanto para IOPS como para MB/s. Esto te permite determinar si la demanda viene determinada por patrones de acceso con un uso intensivo de lectura, de escritura o una combinación de ambos.

5. Utiliza el selector de componentes para activar o desactivar las métricas que desees examinar:
   - **IOPS de lectura** y **IOPS de escritura** — operaciones por segundo según la dirección de I/O
   - **MB/s de lectura** y **MB/s de escritura** — rendimiento en megabytes por segundo según la dirección de I/O
   - **Otras IOPS** y **Otros MB/s** — metadatos y otras operaciones no relacionadas con los datos
   - **Límite de IOPS de QoS** y **Límite de MB/s de QoS** — límites máximos de la política que solo aparecen cuando el volumen utiliza una política de QoS
   - **Rendimiento en la nube** — MB/s escritos en y leídos desde la nube, se muestra solo para las cargas de trabajo que distribuyen capacidad a la nube a través de FabricPool
6. Pasa el cursor por encima de un pico del gráfico para ver el valor exacto y el desglose porcentual de cada componente en ese momento.

   La información que aparece al pasar el cursor también muestra el tamaño de I/O medio (rendimiento dividido por IOPS) para cada categoría, lo que puede indicar si la carga de trabajo está realizando I/O secuencial de gran tamaño o I/O aleatorio de pequeño tamaño.

7. Activa la opción **Mostrar previsión** para predecir si las tendencias actuales de rendimiento alcanzarán el límite de IOPS o MB/s de QoS.

   Si la línea de previsión se está acercando a una línea límite de QoS, es posible que ONTAP limite la carga de trabajo en breve.

8. Si quieres ver la demanda agregada sin el desglose, abre el menú desplegable **Ver** y selecciona **Totales**.

   La vista de totales muestra una única línea de IOPS y una única línea de MB/s, lo que resulta útil para obtener un resumen rápido de la demanda general.

Después de que termines

Utiliza los patrones de rendimiento que observes para decidir qué hacer a continuación:

- Si las IOPS de lectura son muy elevadas en comparación con las de escritura, plantéate si la configuración de lectura anticipada o el almacenamiento en caché pueden reducir la carga sobre el volumen.
- Si la carga de trabajo se está acercando o ha alcanzado el límite de IOPS o MB/s de QoS, usa las líneas de límite de QoS y las definiciones de métricas relacionadas para confirmar la limitación y decidir si necesitas ajustar el límite.
- Si el rendimiento es alto y la latencia también es elevada, consulta la sección **Utilización de recursos** para determinar si el nodo o el agregado subyacente está en contención. Compara los picos de rendimiento, los picos de latencia y la utilización de recursos durante el mismo periodo.

- Si el analizador muestra un rápido crecimiento de la capacidad o de las instantáneas mientras la demanda va en aumento, revisa las métricas de capacidad y de instantáneas para comprender cómo podría afectar ese crecimiento al volumen.

"Investiga la alta latencia en un volumen". "Aprende sobre las métricas de Workload Analyzer en el despliegue local de NetApp Console".

Investiga el crecimiento de la capacidad en un volumen en una implementación local de NetApp Console

Utiliza Workload Analyzer en la implementación local de NetApp Console para averiguar por qué un volumen se está quedando sin espacio.

Cuando un volumen se esté llenando o las copias de instantáneas estén ocupando más espacio del previsto, comprueba las tendencias de capacidad y de instantáneas a lo largo del tiempo. La sección de análisis de capacidad muestra cómo varían el espacio físico y el espacio disponible, desglosa el ahorro de eficiencia de almacenamiento y prevé cuándo alcanzará el volumen un umbral de capacidad.

Si abres el analizador desde una alerta o desde el inventario de volúmenes, el volumen ya está seleccionado y puedes centrarte en las tendencias de capacidad y la ventana de previsión.

Pasos

1. Abre Workload Analyzer mediante uno de los siguientes métodos:
   - En el menú **Salud**, selecciona **Analizador de carga de trabajo**, luego busca y selecciona el volumen que quieres investigar en el campo **Volumen**.
   - Desde la página **Almacenamiento > Flotas > Inventario**, ve a un volumen que quieras analizar y selecciona **Analizar** en el menú de acciones.
   - En la página **Alertas > Resumen**, selecciona una alerta para el volumen que quieres investigar y luego selecciona **Analizar** en los detalles de la alerta.
2. Establece el **Intervalo de tiempo** para que abarque el periodo de crecimiento de la capacidad y luego selecciona **Analizar**.
3. Desplázate hasta la sección **Análisis de capacidad**.
4. Selecciona **Vista de capacidad** en el menú desplegable **Vista**.

   El gráfico muestra la capacidad física como el área apilada inferior y la capacidad disponible como el área apilada superior. Juntas equivalen al tamaño total del volumen, así que puedes ver qué tan rápido está disminuyendo el espacio disponible.

5. Pasa el cursor por encima de un punto del gráfico para ver el desglose de la eficiencia de almacenamiento, incluyendo el ahorro derivado de la deduplicación, la compresión y la compactación, así como el índice global de eficiencia de almacenamiento.

   Una disminución del índice de eficiencia mientras aumenta la capacidad física puede indicar que los datos recién escritos no se están deduplicando ni comprimiendo tan bien como los datos existentes.

6. Para analizar el consumo de instantáneas, selecciona **Snapshot View** en el menú desplegable **View**.

   El gráfico muestra la reserva de snapshot como una línea de referencia horizontal y la capacidad utilizada por las instantáneas como un área situada debajo de ella. Pasa el cursor por encima para ver el espacio utilizado por las instantáneas y su porcentaje respecto a la reserva, el número total de instantáneas y la antigüedad de la instantánea más antigua.

Cuando el consumo de instantáneas supera la reserva, las instantáneas comienzan a ocupar espacio en el área de datos del volumen, lo que reduce el espacio disponible para nuevas escrituras.

7. Si el volumen almacena datos en la nube, selecciona **Vista de niveles de la nube** en el menú desplegable **Ver** para comparar la capacidad disponible en el nivel de rendimiento local con la del nivel de capacidad en la nube.
8. Activa **Mostrar previsión** para predecir cuándo el volumen alcanzará un umbral de capacidad de advertencia o crítico.

   La previsión de capacidad requiere al menos 10 días de datos históricos. Cuando quedan menos de 30 días de capacidad antes de que se llene el volumen, el analizador identifica el almacenamiento como casi lleno. La previsión muestra un mensaje informativo con el tiempo estimado hasta que se alcance el límite.

Después de que termines

Utiliza las tendencias de capacidad que observes para decidir qué hacer a continuación:

- Si la capacidad disponible tiende a agotarse, plantéate aumentar el tamaño del volumen, activar el crecimiento automático o trasladar datos fuera del volumen.
- Si la capacidad utilizada por las instantáneas supera la reserva, revisa tu política de snapshot y la retención para recuperar espacio.
- Si el índice de eficiencia del almacenamiento está disminuyendo, revisa si el tipo de datos de la carga de trabajo o la configuración de eficiencia en línea están reduciendo el ahorro. Usa "Aprende sobre las métricas de Workload Analyzer en el despliegue local de NetApp Console" para descripciones detalladas de las métricas de capacidad, instantáneas y eficiencia.

Métricas de Workload Analyzer en la implementación local de NetApp Console

En una implementación local de NetApp Console, el Workload Analyzer muestra métricas en seis secciones. La descripción de cada métrica explica cómo el analizador muestra la métrica en el gráfico y qué indica sobre el comportamiento del volumen.

Líneas de referencia de QoS en los gráficos de latencia

Si el volumen seleccionado utiliza una política de calidad de servicio (QoS), puedes utilizar dos líneas de referencia adicionales en el selector de métricas:

Línea de referencia	Descripción
Límite máximo de QoS	El límite máximo de latencia definido por la política de calidad de servicio (QoS). Cuando la línea de latencia se aproxima o toca esta línea, ONTAP está limitando la carga de trabajo, y el límite de QoS, en lugar de un recurso físico, es la principal fuente de latencia.
Límite mínimo de QoS	El límite mínimo garantizado de latencia definido por la política de QoS. Esta línea indica el piso de tiempo de respuesta que se aplica a la carga de trabajo. Cuando otras cargas de trabajo utilizan los valores mínimos de QoS para garantizar su rendimiento, ONTAP puede limitar esta carga de trabajo, lo que provoca que presente una mayor latencia.

Estas líneas horizontales no aparecen en el desglose del centro de retardo al pasar el cursor por encima. Sirven como umbrales de referencia, no como factores que contribuyen a la latencia.

Desglose de la latencia por tipo de I/O

Utiliza el desglose por tipo de I/O en la sección **Análisis de latencia** después de seleccionar **Desglose por centro de retardo** en el menú desplegable Ver. El gráfico desglosa la latencia total en tres categorías según la dirección de la operación de I/O. Utiliza estas métricas para determinar si un problema de rendimiento está afectando las operaciones de lectura, escritura o metadatos.

Tipo de latencia	Descripción	Causas habituales de los valores elevados
Latencia de lectura	Tiempo medio que tarda en completarse una solicitud de lectura de un cliente en el volumen, desde el momento en que se recibe la solicitud hasta que se devuelven los datos. Las solicitudes de lectura deben recorrer la ruta completa de I/O, desde la capa de protocolo de red, pasando por la pila de procesamiento de datos, hasta el agregado donde residen los datos.	Contendencia de agregados o de discos; fallos de caché que provocan lecturas en el disco físico; datos inactivos recuperados de un nivel de capacidad en la nube a través de FabricPool; lecturas entre nodos cuando los datos residen en un nodo distinto al que gestiona la solicitud.
Latencia de escritura	Tiempo medio de confirmación de una solicitud de escritura de un cliente en el volumen. ONTAP confirma una escritura una vez que se ha registrado en el registro de escritura de la NVRAM; los datos se transfieren al agregado más tarde.	Saturación de la NIC o alta latencia de ida y vuelta entre el cliente y el nodo de almacenamiento; SnapMirror sincrónico esperando a que el clúster de destino confirme la recepción antes de que se pueda confirmar la escritura; presión sobre la NVRAM bajo cargas intensas de escritura; sobrecarga de CPU por deduplicación, compresión o compactación en línea que se ejecutan en la ruta de I/O de escritura.
Otra latencia	Tiempo medio necesario para completar operaciones que no sean de lectura ni de escritura en el volumen, incluyendo aperturas de archivos, consultas de atributos, recorridos de directorios, creaciones de archivos y bloqueos. Una latencia elevada en otros aspectos puede afectar la capacidad de respuesta de la aplicación incluso cuando la latencia de lectura y escritura parece normal.	Presión sobre la CPU debido a operaciones de eficiencia en línea que compiten con el procesamiento de metadatos; alta actividad en el espacio de nombres por cargas de trabajo que generan grandes cantidades de creaciones y eliminaciones de archivos o análisis de directorios; limitación de QoS que restringe el total de IOPS, dejando menos IOPS disponibles para operaciones de metadatos; sobrecarga de activación de volúmenes cuando muchos volúmenes están activos al mismo tiempo.

Componentes del rendimiento

Utiliza los componentes de rendimiento de la sección **Análisis de rendimiento** después de seleccionar **Desglose (RWO)** en el menú desplegable **Ver**. El analizador muestra simultáneamente tanto las IOPS como los MB/s.

Componente	Descripción	Se traduce como
IOPS de lectura	Operaciones de lectura por segundo.	Área apilada en el gráfico de IOPS.

Componente	Descripción	Se traduce como
IOPS de escritura	Operaciones de escritura por segundo.	Área apilada en el gráfico de IOPS.
Otros IOPS	Metadatos y otras operaciones no relacionadas con datos por segundo.	Área apilada en el gráfico de IOPS.
Lectura MB/s	Rendimiento de lectura en megabytes por segundo.	Área apilada en el gráfico de MB/s.
Escritura MB/s	Velocidad de escritura en megabytes por segundo.	Área apilada en el gráfico de MB/s.
Rendimiento de la nube	Ancho de banda en megabytes por segundo entre el volumen y el nivel de capacidad en la nube. Esta métrica solo aparece para las cargas de trabajo que asignan capacidad a la nube a través de FabricPool.	Área apilada en el gráfico de MB/s.

Los componentes de lectura, escritura y otros suman el valor total de IOPS o MB/s. Pasa el cursor por encima del gráfico para ver el valor de cada componente, su porcentaje respecto al total y el tamaño medio de I/O (MB/s ÷ IOPS) por categoría.

Métricas de utilización de recursos

Utiliza la sección **Utilización de recursos** para consultar las métricas de utilización de recursos. El analizador muestra cada recurso que da servicio al volumen en una línea independiente. Los recursos no se superponen.

Métricas de los nodos

Métrica	Descripción
Utilización de nodos	Porcentaje de utilización combinada del nodo. Pasa el cursor por encima para ver la utilización de CPU, la utilización de red y el margen disponible para cada nodo.
Utilización de CPU	Porcentaje de la capacidad de CPU del nodo en uso. La información al pasar el cursor muestra este valor.
Utilización de red	Porcentaje de la capacidad de red del nodo en uso. La información al pasar el cursor muestra este valor.
Espacio libre	Capacidad restante del nodo disponible para cargas de trabajo adicionales. La información que aparece al pasar el cursor por encima muestra este valor.

Métricas agregadas

Métrica	Descripción
Utilización global	Porcentaje de ocupación del disco para el agregado. Pasa el cursor por encima para ver el valor de ocupación del disco, el número de volúmenes del agregado y el margen disponible.
Disco ocupado	Porcentaje de tiempo durante el cual los discos del agregado prestan servicio de I/O de forma activa. La información que aparece al pasar el cursor por encima muestra este valor.

Métrica	Descripción
Recuento de volúmenes	Número de volúmenes alojados actualmente en el agregado. La información que aparece al pasar el cursor por encima muestra este valor.
Espacio libre	Capacidad restante del agregado disponible para una carga de trabajo adicional. La información que aparece al pasar el cursor por encima muestra este valor.

Cuando la línea de utilización de un nodo o un agregado supera el umbral de advertencia de alta utilización, que en el gráfico se indica con una línea de referencia discontinua, es posible que otras cargas de trabajo de ese recurso estén compitiendo con el volumen seleccionado por la capacidad de I/O.

Métricas de capacidad

Vista de capacidad

Utiliza la sección **Análisis de capacidad** para consultar las métricas de **Vista de capacidad** después de seleccionar **Vista de capacidad** en el menú desplegable Vista.

Métrica	Descripción
Capacidad física	Espacio ocupado en el disco tras las operaciones de eficiencia del almacenamiento. Esta es la zona inferior apilada en el gráfico. El espacio físico más el disponible siempre equivalen al tamaño total del volumen.
Capacidad disponible	Espacio libre restante en el volumen. Esta es la zona superior apilada en el gráfico. Disminuye a medida que crece la capacidad física.
Índice de eficiencia de almacenamiento	Índice de eficiencia global (datos lógicos ÷ datos físicos). La información que aparece al pasar el cursor por encima muestra este valor. Refleja el ahorro combinado de la deduplicación, la compresión y la compactación.
Ahorro gracias a la deduplicación	Espacio ahorrado al eliminar bloques de datos duplicados. La información que aparece al pasar el cursor por encima muestra este valor.
Ahorro por compresión	Espacio ahorrado gracias a la compresión de datos en línea. La información que aparece al pasar el cursor por encima muestra este valor.
Ahorro en la compactación	Espacio ahorrado al agrupar varios bloques pequeños en un único bloque físico. La información que aparece al pasar el cursor por encima muestra este valor.

Vista de snapshot

Utiliza la vista Snapshot cuando quieras consultar métricas específicas de las instantáneas.

Métrica	Descripción	Se traduce como
Instantánea disponible	Espacio preasignado reservado para instantáneas, configurado como un porcentaje del tamaño del volumen.	Línea de referencia horizontal.
Instantánea utilizada	Espacio real ocupado por las copias de instantáneas.	Gráfico de área por debajo de la línea de reserva.

Pasa el cursor por encima del gráfico para ver el tamaño de la reserva de snapshot, el espacio utilizado por las instantáneas y su porcentaje respecto a la reserva, el número total de instantáneas y la antigüedad de la instantánea más antigua. Cuando el consumo de instantáneas supera la reserva, las instantáneas comienzan

a ocupar espacio en el área de datos del volumen.

Comportamiento previsto

Utiliza el botón de activación/desactivación **Mostrar previsión** en cualquier sección de análisis cuando quieras proyectar valores futuros más allá del momento actual basándote en la tendencia observada. Los siguientes comportamientos se aplican a todas las secciones:

Aspecto	Comportamiento
Ventana de proyección	Realiza proyecciones hacia el futuro en función del intervalo de tiempo seleccionado. Para una vista de 2 horas, la ventana de proyección es de aproximadamente 1 hora. Para una vista de 7 días, la ventana de proyección se extiende varios días.
Estilo visual	El analizador muestra los valores previstos mediante una línea discontinua. Un separador vertical marca el límite entre los datos reales y los valores previstos.
Alertas de umbral	El analizador muestra un mensaje de aviso cuando la previsión indica que el volumen superará un umbral de advertencia o crítico, junto con el tiempo estimado para que ocurra el rebasamiento.
Base de la tendencia	La proyección utiliza la tasa de cambio del tramo más reciente del intervalo de tiempo seleccionado. La elevada volatilidad de los datos recientes reduce la fiabilidad de la previsión.
Datos mínimos necesarios	La previsión de capacidad requiere al menos 10 días de datos históricos. Cuando quedan menos de 30 días de capacidad antes de que se llene el volumen, el analizador identifica el almacenamiento como casi lleno.

Información relacionada

- "Obtén información sobre Workload Analyzer para el despliegue local de NetApp Console"
- "Investiga la alta latencia en un volumen"
- "Investiga la demanda de alto rendimiento en un volumen"
- "Investiga el crecimiento de la capacidad en un volumen"

Administra y supervisa la implementación local de NetApp Console

Infórmate sobre la administración y la supervisión en la implementación local de NetApp Console

Después de implementar el despliegue local de NetApp Console, usa las herramientas de administración y monitoreo para revisar la actividad, mantener la máquina virtual y gestionar el acceso de los miembros.

Actividad de auditoría

Revisa la actividad de los usuarios y de la API, realiza un seguimiento del estado de las operaciones de la NetApp Console, descarga los registros de auditoría y exporta los registros a herramientas externas cuando necesites un periodo de conservación más largo o un análisis adicional.

- "Audita la actividad de implementación local de NetApp Console"
- "Configura los canales de entrega de notificaciones en la implementación local de NetApp Console"

Licenses and subscriptions

Utiliza la información sobre licencias y suscripciones para conocer los derechos de acceso a los servicios y el estado de las suscripciones de tu entorno de Console.

"Más información sobre Licenses and subscriptions".

Mantén y soluciona problemas de la máquina virtual de implementación local de la NetApp Console

Realiza el mantenimiento de la máquina virtual que aloja la implementación local de Console, revisa la configuración de red y del sistema, accede a las herramientas de diagnóstico y soluciona problemas cuando el servicio o el agente no funcionan como esperas.

"Realiza el mantenimiento de tu vCenter o host ESXi para la implementación local de Console".

Gestiona usuarios y accesos

Revisa el acceso de los miembros en toda tu organización, ajusta el acceso a nivel de flota y gestiona la configuración de seguridad, como la recuperación de MFA y las credenciales de cuentas de servicio.

- "Gestiona el acceso de los miembros en NetApp Console"
- "Ver o cambiar las asignaciones de acceso a la flota en la implementación local de NetApp Console"
- "Gestiona la seguridad de los miembros en la implementación local de NetApp Console"

Audita la actividad de implementación local de NetApp Console

Puedes auditar la actividad de los usuarios iniciada tanto desde la interfaz de usuario como desde la API en la página de Auditoría, y puedes supervisar el estado de las operaciones en la implementación local de NetApp Console y el usuario que las inició.

Roles requeridos

Superadministrador, administrador de la organización, administrador de carpetas y flotas, analista de soporte de operaciones, supervisor, visor de la organización o visor de carpetas y flotas. "Conoce los roles de acceso".

Puedes consultar la actividad de auditoría en la implementación local de la Console, descargar un archivo CSV con los registros de auditoría o configurar el envío de dichos registros a tu propio servidor syslog mediante un webhook.

Audita la actividad de los usuarios desde la página Auditoría

Utiliza la página de Auditoría para identificar quién realizó una acción o su estado.

La página «Auditoría» muestra las acciones que los usuarios han realizado dentro de tu organización. Por ejemplo, puedes comprobar quién añadió un miembro a una organización o que una flota se eliminó correctamente, así como ver otras acciones de gestión de almacenamiento que los usuarios realizaron en tu organización.

Los registros de auditoría muestran la actividad de los siguientes servicios:

- Tenancy: acciones relacionadas con la gestión de tu organización, como añadir usuarios, crear flotas y asociar recursos.
- Gestión del almacenamiento: acciones relacionadas con la gestión de tus recursos de almacenamiento.
- Federación: acciones relacionadas con la gestión de federaciones, como crear federaciones y agregar o eliminar organizaciones federadas.

Pasos

1. Selecciona **Administración > Auditoría**.
2. Utiliza los filtros situados encima de la tabla para cambiar qué acciones se muestran en la tabla.

   Por ejemplo, puedes utilizar el filtro **Servicio** para mostrar las acciones relacionadas con un servicio concreto, o puedes utilizar el filtro **Usuario** para mostrar las acciones relacionadas con una cuenta de usuario concreta.

Filtra los registros de auditoría para las acciones de gestión de identidades y acceso

Para ver únicamente las acciones relacionadas con la gestión de tu organización, como añadir miembros, crear flotas o eliminar recursos, filtra el registro de auditoría por el servicio Tenancy.

Pasos

1. Selecciona **Administración > Auditoría**.
2. Utiliza los filtros para acotar los resultados. Selecciona **Service** y luego selecciona **Tenancy**.
3. Utiliza cualquiera de los demás filtros para refinar aún más los resultados.

   Por ejemplo, utiliza el filtro **Usuario** para mostrar las acciones de IAM realizadas por una cuenta de usuario concreta.

Descarga los registros de auditoría desde la página de Auditoría

Puedes descargar los registros de auditoría desde la página de Auditoría a un archivo CSV. Esto te permite mantener un registro de las acciones que realizan los usuarios en tu organización. El archivo CSV descargado incluye todas las columnas del registro de auditoría, independientemente de los filtros o de las columnas que se muestren en la página de Auditoría.

Pasos

1. En la página **Audit**, selecciona el icono de descarga situado en la esquina superior derecha de la tabla.

Mantén NetApp Console

Realiza el mantenimiento de tu vCenter o host ESXi para la implementación local de NetApp Console

En una implementación local de NetApp Console, puedes realizar cambios en tu VCenter o host ESXi existentes después de implementar la Console local deployment. Por ejemplo, puedes aumentar la CPU o la RAM de la instancia de VM que aloja la Console local deployment.

Realiza estas tareas de mantenimiento mediante la consola web de la VM:

- Aumentar el tamaño del disco

- Reinicia la implementación local de la consola
- Actualizar rutas estáticas
- Actualizar dominios de búsqueda

Limitaciones

Sólo puedes ver (no actualizar) la información sobre la dirección IP, DNS y gateways a través de la consola de mantenimiento.

Accede a la consola de mantenimiento de la VM

Puedes acceder a la consola de mantenimiento desde el cliente vSphere.

Pasos

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de la Console.
3. Selecciona **Launch Web Console**.
4. Inicia sesión en la instancia de VM con el nombre de usuario y la contraseña que especificaste al crear la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste al crear la instancia de VM.

Cambia la contraseña del usuario «maint»

Puedes cambiar la contraseña para el usuario `maint`.

Pasos

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de la Console.
3. Selecciona **Launch Web Console**.
4. Inicia sesión en la instancia de VM con el nombre de usuario y la contraseña que especificaste al crear la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste al crear la instancia de VM.
5. Introduce `1` para ver el menú `System Configuration`.
6. Accede a `1` para cambiar la contraseña del usuario de mantenimiento y sigue las instrucciones que aparecen en pantalla.

Aumenta la CPU o la RAM de la instancia de VM

Puedes aumentar la CPU o la RAM de la instancia de VM que aloja la implementación local de Console.

Modifica la configuración de la instancia de VM en tu VCenter o en el host ESXi y luego usa la consola de mantenimiento para aplicar los cambios.

Pasos en el cliente vSphere

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de la Console.
3. Haz clic con el botón derecho del ratón en la instancia de VM y selecciona **Editar configuración**.
4. Aumenta el espacio en el disco duro usado para /opt o la partición /var.

a. Selecciona **Hard Disk 2** para aumentar el espacio en disco destinado a /opt.

b. Selecciona **Disco duro 3** para aumentar el espacio en disco usado para /var.

5. Guarda tus cambios.

Pasos en la consola de mantenimiento

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de Console.
3. Selecciona **Launch Web Console**.
4. Inicia sesión en la instancia de VM con el nombre de usuario y la contraseña que especificaste al crear la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste al crear la instancia de VM.
5. Entra al menú `1 to view the `System Configuration`.
6. Introduce `2` y sigue las instrucciones que aparecen en pantalla. La consola busca nuevas configuraciones y aumenta el tamaño de las particiones.

Ver la configuración de red de la VM de implementación local de la NetApp Console

Consulta la configuración de red de la máquina virtual de implementación local de la Console en el cliente VSphere para confirmar o solucionar problemas de red. Solo puedes consultar (no modificar) los siguientes parámetros de red: dirección IP y detalles de DNS.

Pasos

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de la Console.
3. Selecciona **Launch Web Console**.
4. Inicia sesión en la instancia de VM con el nombre de usuario y la contraseña que especificaste al crear la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste al crear la instancia de VM.
5. Introduce `2` para ver el menú `Network Configuration`.
6. Introduce un número entre 1 y 6 para ver la configuración de red correspondiente.

Actualiza las rutas estáticas de la VM de implementación local de Console

Agrega, actualiza o elimina rutas estáticas para la VM de implementación local de la NetApp Console según sea necesario.

Pasos

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de la Console.
3. Selecciona **Launch Web Console**.
4. Inicia sesión en la instancia de VM con el nombre de usuario y la contraseña que especificaste al crear la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste al crear la instancia de VM.
5. Introduce `2` para ver el menú `Network Configuration`.
6. Introduce `7` para actualizar las rutas estáticas y sigue las instrucciones que aparecen en pantalla.

7. Pulsa Intro.
8. Opcionalmente, haz cambios adicionales.
9. Escribe `9` para guardar los cambios.

Actualizar la configuración de búsqueda de dominios para la VM de implementación local de la Console

Puedes actualizar la configuración del dominio de búsqueda de la VM de implementación local de la Console.

Pasos

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de la Console.
3. Selecciona **Launch Web Console**.
4. Inicia sesión en la instancia de VM con el nombre de usuario y la contraseña que especificaste al crear la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste al crear la instancia de VM.
5. Introduce `2`` para ver el menú `Network Configuration`.
6. Accede a `8` para actualizar la configuración de búsqueda de dominios y sigue las instrucciones que aparecen en pantalla.
7. Pulsa Intro.
8. Opcionalmente, haz cambios adicionales.
9. Escribe `9` para guardar los cambios.

Accede a las herramientas de diagnóstico de la implementación local de la consola

Accede a las herramientas de diagnóstico para solucionar problemas con la implementación local de la Console. NetApp Support puede pedirte que hagas esto al solucionar problemas.

Pasos

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de la Console.
3. Selecciona **Launch Web Console**.
4. Inicia sesión en la instancia de VM con el nombre de usuario y la contraseña que especificaste al crear la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste al crear la instancia de VM.
5. Escribe `3` para ver el menú de Soporte y diagnóstico.
6. Introduce `1` para acceder a las herramientas de diagnóstico y sigue las indicaciones en pantalla.

Accede de forma remota a las herramientas de diagnóstico de la implementación local de la consola

Puedes acceder a las herramientas de diagnóstico de forma remota mediante una herramienta como Putty. Activa el acceso SSH a la VM de implementación local de la Console asignando una contraseña de un solo uso.

El acceso SSH permite utilizar funciones avanzadas del terminal, como copiar y pegar.

Pasos

1. Abre el cliente vSphere e inicia sesión en tu vCenter.
2. Selecciona la instancia de VM que aloja la implementación local de la Console.
3. Selecciona **Launch Web Console**.
4. Inicia sesión en la instancia de VM con el nombre de usuario y la contraseña que especificaste al crear la instancia de VM. El nombre de usuario es `maint` y la contraseña es la que especificaste al crear la instancia de VM.
5. Introduce `3` para ver el menú `Support and Diagnostics`.
6. Accede a `2` para utilizar las herramientas de diagnóstico y sigue las instrucciones que aparecen en pantalla para configurar una contraseña de un solo uso que caduca en 24 horas.
7. Utiliza una herramienta SSH, como Putty, para conectarte a la máquina virtual de implementación local de Console con el nombre de usuario `diag` y la contraseña de un solo uso que configuraste.

Gestiona usuarios y accesos

Gestiona el acceso de los miembros en la implementación local de NetApp Console

En una implementación local de NetApp Console, revisa o modifica los roles de un usuario en varias carpetas o flotas, como comprobar todo a lo que puede acceder un ingeniero de almacenamiento, añadir un nuevo rol en otra región o retirar el acceso de ese usuario cuando cambien sus responsabilidades.

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".

Puedes consultar y gestionar el acceso de dos formas según tus necesidades. Si quieres ver los roles que tiene un usuario en particular en toda la flota de tu organización, usa la página **Members**.

Si quieres comprobar quién puede acceder a una flota concreta, consulta los miembros asignados a dicha flota. "Gestiona las asignaciones de acceso a la flota".

Para añadir un nuevo miembro, una cuenta de servicio o un usuario de directorio y asignarle su primer rol, utiliza la tarea de incorporación. "Agregar miembros y asignar roles".

Entiende cómo se concede el acceso en NetApp Console

La NetApp Console utiliza el control de acceso basado en roles (RBAC) para gestionar los permisos de los miembros. Puedes asignar roles predefinidos a nivel de organización, carpeta o flota, en función del ámbito de acceso que necesite cada miembro.

Uso de la herencia de roles

Un rol que asignas a nivel de organización o de carpeta se hereda en los ámbitos subordinados, así que cambia una asignación heredada en el ámbito superior donde la concediste originalmente.

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

Ver los roles asignados a un miembro

Confirma exactamente qué roles tiene un miembro y en qué ámbito antes de hacer un cambio. Por ejemplo, comprueba si un compañero de equipo ya tiene el rol de Storage admin en la `Production-EU-West` fleet.

Si tienes el rol de *Folder or fleet admin*, la página muestra a todos los miembros de la organización. Sin embargo, solo puedes ver y gestionar los permisos de las carpetas y flotas que administras. "Infórmate sobre las acciones de los administradores de carpetas o de flotas en la implementación local de NetApp Console".

1. Desde la página **Miembros**, busca a un miembro en la tabla, selecciona ••• y luego selecciona **Ver detalles**.
2. En la tabla, despliega la fila correspondiente a la organización, carpeta o flota en la que quieras ver el rol asignado al miembro y selecciona **Ver** en la columna **Role**.

Asignar o modificar el acceso de los miembros

Puedes ajustar el acceso de un miembro siempre que cambien sus responsabilidades. Por ejemplo, cuando un compañero de equipo asume tareas de backup para una segunda región, añade el rol de Backup and Recovery admin en la flota de esa región sin modificar sus roles de almacenamiento actuales.

Si necesitas añadir un nuevo miembro y asignarle su primer rol, consulta "Agregar miembros y asignar roles".

Agrega un rol de acceso a un miembro existente

Asigna a un miembro un rol adicional a nivel de organización, carpeta o flota cuando sus responsabilidades se amplíen. Por ejemplo, asigna a un Storage admin el rol de Backup and recovery admin a nivel de organización para que pueda gestionar las tareas de backup and recovery en todas las flotas sin perder sus permisos de almacenamiento actuales.

Puedes asignar a un miembro un rol de acceso para tu organización, carpeta o flota.

Los miembros pueden desempeñar múltiples roles dentro de una misma flota y en diferentes flotas. Por ejemplo, las organizaciones más pequeñas pueden asignar todos los roles de acceso disponibles al mismo usuario, mientras que las organizaciones más grandes pueden encargar a los usuarios tareas más especializadas. Como alternativa, también podrías asignar a un usuario el rol de administrador de resiliencia frente al ransomware a nivel de organización. En ese ejemplo, el usuario podría realizar tareas de resiliencia frente al ransomware en todas las flotas de tu organización.

Tu estrategia de roles de acceso debe ajustarse a la forma en que has organizado tus recursos de NetApp.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Miembros**.
3. Selecciona una de las pestañas de miembros: **Usuarios**, **Usuarios del directorio** o **Cuentas de servicio**.
4. Selecciona el menú de acciones ••• junto al miembro al que quieres asignar un rol y selecciona **Add a role**.
5. Para añadir un rol, sigue los pasos que se indican en el cuadro de diálogo:
   - **Selecciona una organización, carpeta o flota**: Elige el nivel de la jerarquía de recursos para el que el miembro debe tener permisos.

     Si seleccionas la organización o una carpeta, el miembro tendrá permisos para todo lo que se encuentre dentro de la organización o carpeta.

- **Selecciona una categoría**: elige una categoría de función. "Conoce los roles de acceso".
- Selecciona un **rol**: elige un rol que otorgue al miembro permisos para los recursos que están asociados con la organización, la carpeta o la flota que seleccionaste.
- **Añadir función**: Si quieres conceder acceso a carpetas o flotas adicionales dentro de tu organización, selecciona **Añadir función**, especifica otra carpeta o flota o categoría de función y luego selecciona una categoría de función y la función correspondiente.

6. Selecciona **Add new roles**.

Cambiar el rol asignado a un miembro

Sustituye el rol actual de un miembro por otro diferente cuando cambien sus responsabilidades. Por ejemplo, cuando un Storage viewer en la `Production-US-East` fleet necesite el rol de Storage admin en su lugar.

> Cada usuario debe tener al menos un rol. No puedes eliminar todos los roles de un usuario. Si necesitas eliminar todos los roles, elimina al usuario de tu organización.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Miembros**.
3. Selecciona una de las pestañas de miembros: **Usuarios**, **Usuarios del directorio** o **Cuentas de servicio**.
4. Desde la página **Miembros**, busca a un miembro en la tabla, selecciona ••• y luego selecciona **Ver detalles**.
5. En la tabla, despliega la fila correspondiente a la organización, carpeta o flota en la que desees modificar el rol asignado al miembro y selecciona **Ver** en la columna **Rol** para ver los roles asignados a este miembro.
6. Puedes cambiar un rol existente de un miembro o eliminar un rol.
   a. Para cambiar el rol de un miembro, selecciona **Cambiar** junto al rol que quieres cambiar. Solo puedes cambiar un rol por otro dentro de la misma categoría de roles. Por ejemplo, puedes cambiar de un rol de servicio de datos a otro. Confirma el cambio.
   b. Para desasignar un rol a un miembro, selecciona 🗑 junto al rol para desasignar al miembro el rol correspondiente. Se te pedirá que confirmes la eliminación.

Eliminar a un miembro de tu organización

Elimina a un miembro cuando abandone la organización o cambie de función de tal forma que ya no necesite acceso a la Console. Por ejemplo, cuando finaliza el contrato de un colaborador externo o cuando un empleado se traslada a un equipo ajeno a tu organización de la Console.

> **Usuarios del directorio**
>
> Al eliminar a un usuario de tu directorio, se impide que dicho usuario pueda autenticarse. También debes eliminar al usuario de tu organización en Console para mantener la lista de miembros actualizada y eliminar cualquier rol que se le haya asignado en la implementación local de Console.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Miembros**.

3. Selecciona una de las pestañas de miembros: **Usuarios**, **Usuarios del directorio** o **Cuentas de servicio**.
4. Desde la página **Miembros**, busca a un miembro en la tabla, selecciona ••• y luego selecciona **Eliminar usuario**.
5. Confirma que deseas eliminar al miembro de tu organización.

Ver o cambiar las asignaciones de acceso a la flota en la implementación local de NetApp Console

Audita o cambia las asignaciones de acceso de los miembros para carpetas y parques de almacenamiento en la implementación local de NetApp Console. Los administradores de carpetas y parques suelen trabajar desde esta vista porque solo muestra los ámbitos que administran.

Roles de acceso necesarios

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

Como alternativa, puedes gestionar todos los roles de un miembro concreto en varias carpetas o flotas. "Gestiona el acceso de los miembros".

Cómo funciona el acceso a las carpetas y a la flota

La implementación local de Console utiliza el control de acceso basado en roles (RBAC). Un rol que asignes a nivel de carpeta se aplica a todas las flotas y subcarpetas dentro de esa carpeta; un rol que asignes a nivel de flota se aplica solo a los recursos de esa flota. "Conoce la herencia de roles en la implementación local de NetApp Console".

> No puedes cambiar un rol a nivel de flota si un miembro lo hereda de una carpeta o de la organización. Para cambiar el acceso heredado, cambia el rol en el ámbito superior.

Ver los miembros asignados a una carpeta o flota

Comprueba exactamente quién puede gestionar una carpeta o una flota concreta. Por ejemplo, antes de asociar un nuevo clúster ONTAP de producción con la `Production-US-East` flota, abre la pestaña de Acceso de la flota para confirmar quién tiene acceso.

Pasos

1. Selecciona **Administración** > **Identidad y acceso**.
2. Selecciona **Organization**.
3. Desde la página de Organization, navega hasta una carpeta o flota en la tabla, selecciona ••• y luego selecciona **Editar carpeta** o **Editar flota**.
4. Selecciona **Acceso** para ver los miembros que tienen acceso a la carpeta o flota.

Modificar el acceso de los miembros desde una carpeta o una flota

Modifica los roles de los miembros que ya forman parte de tu organización, limitándolos a una sola carpeta o flota. Por ejemplo, cuando un compañero de equipo pasa de una flota de desarrollo a una flota de producción, asciéndelo de Storage viewer a Storage admin en la flota de producción sin afectar su acceso en otros lugares.

Para añadir a un nuevo miembro y asignarle su primer rol, utiliza la tarea de incorporación. "Agregar miembros y asignar roles".

Pasos

1. Desde la página de Organization, navega hasta una carpeta o flota en la tabla, selecciona ••• y luego selecciona **Editar carpeta** o **Editar flota**.
2. Selecciona **Acceso** para ver la lista de miembros que tienen acceso.
3. Modificar el acceso de los miembros:
   - **Cambiar el rol de un miembro**: Para cualquier miembro cuyo rol no sea Organization admin, selecciona su rol actual y elige uno nuevo. El cambio solo se aplica en este ámbito; los roles heredados de un ámbito superior no aparecen aquí.
   - **Eliminar el acceso de un miembro en este ámbito**: para un miembro que tenga un rol definido directamente en esta carpeta o flota, elimina el rol para revocar su acceso en este ámbito. Esto no elimina al miembro de tu organización ni afecta los roles que tenga en otros ámbitos.

     "Eliminar a un miembro de tu organización".
4. Selecciona **Aplicar**.

Gestiona la seguridad de los miembros en la implementación local de NetApp Console

Garantiza el acceso seguro de los usuarios a tu organización de implementación local de NetApp Console gestionando la configuración de seguridad de los miembros. Puedes indicar a los usuarios locales que cambien sus propias contraseñas, gestionar la autenticación multifactor (MFA) de los usuarios locales y volver a generar las credenciales de las cuentas de servicio.

Roles de acceso necesarios

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

Restablecer contraseñas de usuario (solo usuarios locales)

Los administradores no pueden restablecer directamente las contraseñas de los usuarios locales.

Indica a los usuarios locales que restablezcan sus contraseñas desde la página de inicio de sesión de la implementación local de la Console, seleccionando **¿Has olvidado tu contraseña?**.

Esta opción no está disponible para los usuarios de directorio.

Gestiona la autenticación multifactor (MFA) de un usuario local

Si un usuario local pierde el acceso a su dispositivo MFA, puedes eliminar o desactivar su configuración de MFA.

La autenticación multifactor solo está disponible para los usuarios locales. Los usuarios de directorio no pueden habilitar MFA a través de la implementación local de Console.

Sigue estas pautas para elegir la medida adecuada:

- Selecciona **Desactivar** cuando el usuario pierda temporalmente el acceso a su dispositivo MFA. Desactivar MFA permite un inicio de sesión sin MFA durante ocho horas y luego vuelve a activar MFA automáticamente.

- Selecciona **Eliminar** cuando el usuario deba restablecer completamente MFA. Después de que elimines MFA, el usuario inicia sesión sin MFA hasta que la configure de nuevo.

Si un usuario tiene guardado un código de recuperación, puede iniciar sesión con él. Si un usuario no tiene un código de recuperación, desactiva MFA para que pueda iniciar sesión y recuperar el acceso.

Para gestionar la autenticación multifactor de un usuario local, debes tener una dirección de correo electrónico en el mismo dominio que el usuario afectado.

Pasos

1. Selecciona **Administración** > **Identidad y acceso**.
2. Selecciona **Miembros**.
3. Desde la página Miembros, busca a un miembro en la tabla, selecciona ••• y luego selecciona **Gestionar la autenticación multifactor**.
4. Elige si deseas eliminar o desactivar la configuración MFA del usuario.

Después de que termines

Consulta el registro de auditoría para comprobar quién modificó el acceso MFA, cuándo lo hizo y si la acción se completó con éxito. "Descubre cómo auditar la actividad de implementación local de NetApp Console".

Vuelve a generar las credenciales de una cuenta de servicio

Puedes crear nuevas credenciales para una cuenta de servicio si las pierdes o necesitas actualizarlas.

Al crear nuevas credenciales, se eliminan las antiguas. No puedes usar las credenciales antiguas.

Pasos

1. Selecciona **Administración** > **Identidad y acceso**.
2. Selecciona **Miembros**.
3. En la tabla Members, busca una cuenta de servicio, selecciona ••• y luego selecciona **Recrear secretos**.
4. Selecciona **Recrear**.
5. Descarga o copia el client ID y el client secret.

   La implementación local de Console muestra el secreto de cliente solo una vez. Asegúrate de copiarlo o descargarlo y guardarlo en un lugar seguro.

Referencia

NetApp Console API de implementación local

Gestiona tu organización e ID de flota de la implementación local de NetApp Console

En una implementación local de NetApp Console, tu organización de NetApp Console tiene un nombre y un ID. Puedes elegir un nombre para tu organización que te ayude a identificarla. También puede que necesites recuperar el ID de la organización para ciertas integraciones.

Roles de acceso necesarios

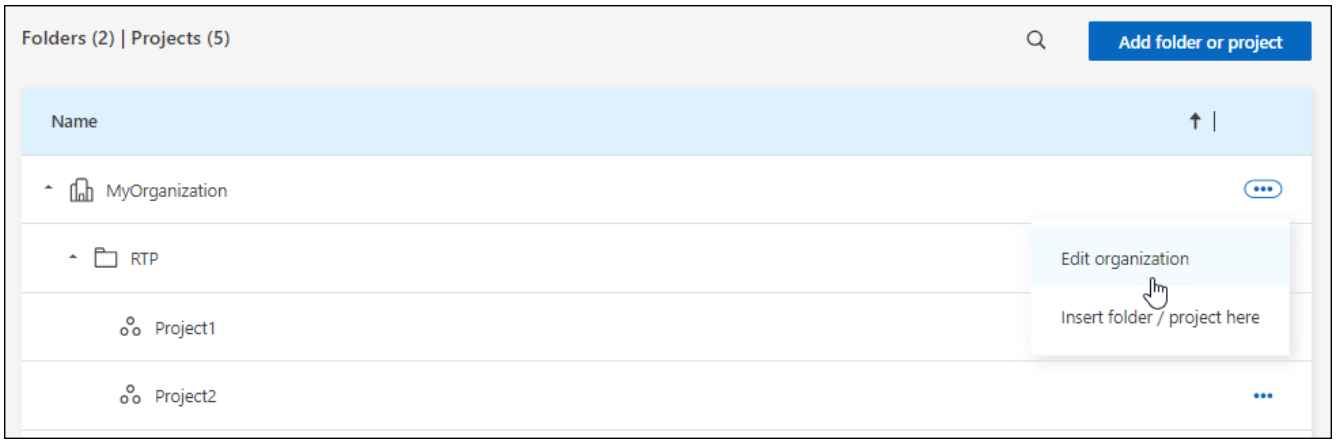
Superadministrador o administrador de la organización. "Conoce los roles de acceso".

Cambia el nombre de tu organización

Puedes cambiar el nombre de tu organización.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Organization**.
3. En la página **Organización**, ve a la primera fila de la tabla, selecciona ••• y luego selecciona **Editar organización**.



4. Introduce un nuevo nombre para la organización y selecciona **Aplicar**.

Obtener el ID de la organización

El identificador de la organización se utiliza para determinadas integraciones con la Console.

Puedes ver el ID de la organización en la página de Organizaciones y copiarlo al portapapeles para lo que necesites.

Pasos

1. Selecciona **Administración > Identidad y acceso** > **Organización**.
2. En la página **Organización**, busca el ID de tu organización en la barra de resumen y cópialo al portapapeles. Puedes guardarlo para usarlo más adelante o copiarlo directamente donde lo necesites.

Obtener el ID de una flota

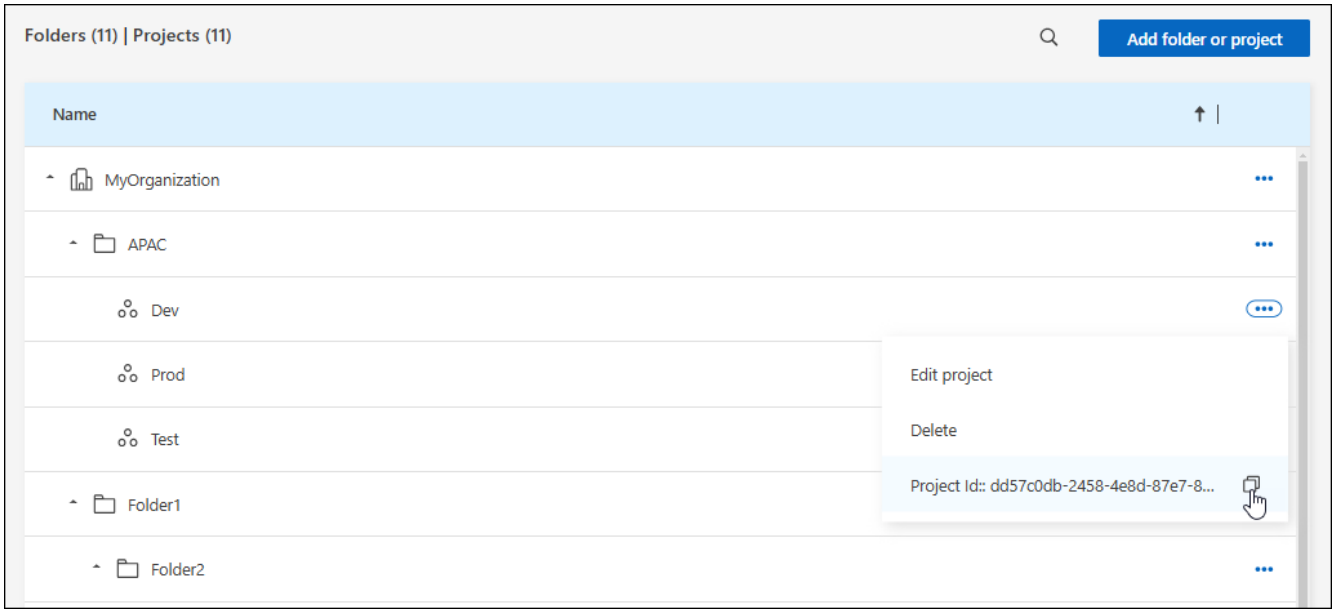
Tendrás que obtener el identificador de una flota si usas la API.

Pasos

1. Desde la página **Organización**, ve a una flota de la tabla y selecciona •••

   Se muestra el identificador de la flota.

2. Para copiar el ID, selecciona el botón copiar.



Información relacionada

- "Conoce la gestión de identidades y control de acceso"
- "Empieza con la identidad y el acceso en NetApp Console"
- "Conoce la API de identidad y acceso"

Proveedores y modelos de LLM compatibles en la implementación local de NetApp Console

La implementación local de NetApp Console es compatible con los tipos de proveedores de LLM de OpenAI, compatibles con OpenAI y de Anthropic. Los modelos que puedes seleccionar dependen del tipo de proveedor y del endpoint que configures.

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.

Elige un modelo que se ajuste a tus requisitos de rendimiento, coste y gobernanza.

Descubre cómo influye el tipo de proveedor en la disponibilidad de los modelos

El tipo de proveedor que elijas determina qué modelos aparecen en la lista de modelos de implementación local de la Console:

- **OpenAI** — ofrece modelos para la integración directa con OpenAI.
- **Compatible con OpenAI** — proporciona los modelos que expone el endpoint compatible de tu organización.
- **Anthropic** — ofrece modelos para la integración directa con Anthropic.

Los modelos que ves pueden variar en función de la configuración del endpoint, el comportamiento del proxy o la gateway y la política de la organización. Los tipos de proveedor varían según el endpoint al que te conectes y los modelos que exponga ese endpoint, no el protocolo de transporte.

Modelos de OpenAI compatibles

- GPT-5.4
- GPT-5.5

Modelos de Anthropic compatibles

- Claude Sonnet 4.6
- Claude Opus 4.6, 4.7 y 4.8

Información relacionada

- "Conecta tu LLM y activa el asistente de NetApp Console".
- "Infórmate sobre la integración de LLM en la implementación local de NetApp Console".

Referencia de alertas de ONTAP en la implementación local de NetApp Console

Esta referencia enumera las alertas de ONTAP que el despliegue local de NetApp Console puede monitorizar, organizadas por categoría de impacto.

Clasificación por gravedad

La misma alerta de EMS puede aparecer como Crítica, Advertencia o Información, dependiendo del evento de ONTAP que la haya provocado:

- **Crítico**: Mapas de las gravedades de ONTAP `alert`, `emergency`
- **Advertencia**: Mapas de gravedad de ONTAP `error`
- **Información**: Mapas de las gravedades de ONTAP `notice`, `informational`
- **Otros**: Pasado tal cual

La asignación dinámica permite que una misma regla de alerta genere diferentes niveles de gravedad según el contexto de ejecución del evento EMS.

En las secciones siguientes se agrupan las alertas por categoría de impacto y cada tabla se ordena alfabéticamente por nombre de alerta.

Alertas de disponibilidad

Estas alertas pueden afectar la disponibilidad del sistema, los servicios o los datos.

Nombre de la alerta	Gravedad	Tipo	Descripción
Conexión con el servidor de Active Directory interrumpida	Crítico	EMS	No se puede acceder a ninguno de los servidores AD/LDAP configurados para este SVM.
El aggregate no está en línea	Crítico	Métrica	Algunos agregados están sin conexión. La creación de volúmenes podría causar FSID duplicados.

Nombre de la alerta	Gravedad	Tipo	Descripción
El servidor antivirus está ocupado	Crítico, Advertencia, Información	EMS	El servidor antivirus está sobrecargado y no puede aceptar más solicitudes de análisis.
Las credenciales de AWS no se han inicializado	Crítico, Advertencia, Información	EMS	Un módulo intentó acceder a las credenciales basadas en roles de AWS IAM antes de que se hubieran inicializado.
No se puede acceder al nivel de la nube	Crítico, Advertencia, Información	EMS	Un nodo de almacenamiento no puede conectarse a la API del almacén de objetos de Cloud Tier. Algunos datos serán inaccesibles.
Fallo del disco	Crítico	Métrica	Un disco ha fallado, se está saneando o está en modo de mantenimiento.
Disco fuera de servicio	Crítico, Advertencia, Información	EMS	Se ha retirado un disco del servicio debido a un fallo, a un proceso de saneamiento o a tareas de mantenimiento.
Se retiró la fuente de alimentación de las estanterías de discos	Crítico, Advertencia, Información	EMS	Se ha retirado una fuente de alimentación de la bandeja de discos.
Se ha superado el límite de comandos del puerto objetivo de FC	Crítico, Advertencia, Información	EMS	El número de comandos pendientes en el puerto objetivo FC físico supera el límite permitido.
Error al devolver el grupo de almacenamiento	Crítico, Advertencia, Información	EMS	Este evento se produce durante la reubicación de un grupo de almacenamiento (agregado) como parte de una reversión de la conmutación por error de almacenamiento (SFO), cuando el nodo de destino no puede acceder a los almacenes de objetos.
Interconexión de alta disponibilidad inactiva	Crítico, Advertencia, Información	EMS	La interconexión de alta disponibilidad (HA) está inactiva. Riesgo de interrupción del servicio cuando no está disponible la conmutación de sitios.
InstanceDown	Crítico	Métrica	La instancia supervisada no es accesible y puede estar inactiva o experimentando problemas de red.
LUN destruido	Crítico, Advertencia, Información	EMS	Se destruyó una LUN y ya no es accesible.

Nombre de la alerta	Gravedad	Tipo	Descripción
LUN fuera de línea	Crítico, Advertencia, Información	EMS	Se desconectó manualmente una LUN.
Fallo del ventilador de la unidad principal	Crítico, Advertencia, Información	EMS	Uno o varios ventiladores de la unidad principal han dejado de funcionar. El sistema sigue funcionando.
El ventilador de la unidad principal está en estado de alerta	Crítico, Advertencia, Información	EMS	Uno o varios ventiladores de refrigeración de la unidad principal están en estado de aviso.
Se ha superado el número máximo de sesiones por usuario	Crítico, Advertencia, Información	EMS	Has superado el número máximo de sesiones permitidas por usuario en una conexión TCP.
Se ha superado el número máximo de veces que se puede abrir un archivo	Crítico, Advertencia, Información	EMS	Has superado el número máximo de veces que puedes abrir el archivo a través de una conexión TCP.
MetroCluster conmutación de sitios automática no planificada desactivada	Crítico, Advertencia, Información	EMS	La función de conmutación de sitios automática no planificada se ha desactivado en este clúster.
MetroCluster monitorización	Crítico, Advertencia, Información	EMS	Se ha detectado una alerta del control del estado del sistema.
Se ha agotado el grupo de almacenamiento de NFSv4	Crítico, Advertencia, Información	EMS	Se ha agotado un pool de almacenamiento NFSv4.
Conflicto de nombres NetBIOS	Crítico, Advertencia, Información	EMS	El servicio de nombres NetBIOS ha recibido una respuesta negativa a una solicitud de registro de nombre de un equipo remoto.
No hay ningún motor de análisis registrado	Crítico, Advertencia, Información	EMS	El conector antivirus notificó a ONTAP que no tiene un motor de análisis registrado.
No hay conexión con Vscan	Crítico, Advertencia, Información	EMS	ONTAP no tiene conexión Vscan para atender las solicitudes de análisis de virus. Esto podría causar indisponibilidad de datos si la opción de análisis obligatorio está activada.

Nombre de la alerta	Gravedad	Tipo	Descripción
Servidor antivirus sin respuesta	Crítico, Advertencia, Información	EMS	ONTAP detectó un servidor antivirus que no respondía y cerró forzosamente su conexión Vscan.
Recurso compartido de administrador inexistente	Crítico, Advertencia, Información	EMS	Problema de Vscan: un cliente ha intentado conectarse a un recurso compartido ONTAP_ADMIN$ que no existe.
La batería de la NVRAM está baja	Crítico, Advertencia, Información	EMS	La capacidad de la batería de la NVRAM es extremadamente baja. Podría producirse una pérdida de datos si la batería se agota.
Espacio de nombres NVMe destruido	Crítico, Advertencia, Información	EMS	Se destruyó un espacio de nombres NVMe y ya no es accesible.
Espacio de nombres NVMe desconectado	Crítico, Advertencia, Información	EMS	Se desconectó manualmente un espacio de nombres NVMe.
Espacio de nombres NVMe en línea	Crítico, Advertencia, Información	EMS	Se ha vuelto a poner en funcionamiento un espacio de nombres NVMe.
Periodo de gracia de la licencia de NVMe-oF activo	Crítico, Advertencia, Información	EMS	Este evento se produce a diario cuando se utiliza el protocolo NVMe over Fabrics (NVMe-oF) y el periodo de gracia de la licencia está activo.
Ha vencido el periodo de gracia de la licencia de NVMe-oF	Crítico, Advertencia, Información	EMS	El periodo de gracia de la licencia de NVMe over Fabrics (NVMe-oF) ha finalizado y la funcionalidad NVMe-oF está desactivada.
Inicio del periodo de gracia de la licencia de NVMe-oF	Crítico, Advertencia, Información	EMS	Se ha detectado la configuración de NVMe over Fabrics (NVMe-oF) durante la actualización al software ONTAP 9.5.
No se puede resolver el host del almacén de objetos	Crítico, Advertencia, Información	EMS	No se puede resolver el nombre de host del servidor del almacén de objetos en una dirección IP.
El LIF entre clústeres del almacén de objetos está inactivo	Crítico, Advertencia, Información	EMS	El cliente del almacén de objetos no puede encontrar un LIF operativo para comunicarse con el servidor del almacén de objetos.

Nombre de la alerta	Gravedad	Tipo	Descripción
Discrepancia en la firma del almacén de objetos	Crítico, Advertencia, Información	EMS	La firma de la solicitud enviada al servidor del almacén de objetos no coincide con la firma calculada por el cliente.
Estado del puerto inactivo	Crítico	EMS	Este puerto Ethernet está inactivo. El tráfico en ese enlace podría verse afectado.
Tiempo de espera de READDIR	Crítico, Advertencia, Información	EMS	Una operación de archivo READDIR ha superado el tiempo de espera permitido para su ejecución en WAFL.
Error al reubicar el grupo de almacenamiento	Crítico, Advertencia, Información	EMS	Este evento se produce durante la reubicación de un grupo de almacenamiento (agregado), cuando el nodo de destino no puede acceder a los almacenes de objetos.
El estado «activo-activo» de SAN ha cambiado	Crítico, Advertencia, Información	EMS	La ruta SAN ya no es simétrica.
No se ha detectado el pulso del Service Processor	Crítico, Advertencia, Información	EMS	ONTAP no está recibiendo la señal de pulso esperada del SP.
Se ha detenido el heartbeat del procesador de servicios	Crítico, Advertencia, Información	EMS	ONTAP ya no recibe señales de actividad del SP.
El procesador de servicios no está configurado	Crítico, Advertencia, Información	EMS	Este evento se produce cada semana para recordarte que debes configurar el procesador de servicios (SP).
Procesador de servicio desconectado	Crítico, Advertencia, Información	EMS	El procesador de servicio (SP) está desconectado.
SFP en el adaptador objetivo FC recibe poca potencia	Crítico, Advertencia, Información	EMS	Esta alerta se produce cuando la potencia recibida (RX) por un transceptor enchufable de factor de forma pequeño (SFP en FC objetivo) está en un nivel por debajo del umbral definido.
SFP en adaptador objetivo FC transmitiendo a baja potencia	Crítico, Advertencia, Información	EMS	Esta alerta se produce cuando la potencia transmitida (TX) por un transceptor enchufable de factor de forma pequeño (SFP en FC target) se encuentra por debajo del umbral definido.
Error al crear una copia en la sombra	Crítico, Advertencia, Información	EMS	Un Servicio de copias en la sombra de volumen (VSS), una operación del servicio de copia de seguridad y restauración de Microsoft Server, ha fallado.

Nombre de la alerta	Gravedad	Tipo	Descripción
Se ha averiado el ventilador de la estantería	Crítico, Advertencia, Información	EMS	El ventilador o módulo de ventilación indicado de la estantería ha fallado.
SnapMirror el tiempo de retraso es alto	Crítico	Métrica	La relación SnapMirror lleva más de una hora de retraso respecto al horario previsto de actualización.
Interconexión de alta disponibilidad del almacenamiento: uno o más enlaces inactivos	Advertencia	EMS	Uno o varios enlaces de interconexión de alta disponibilidad con el nodo asociado están inactivos. La redundancia de conmutación de sitios se reduce.
Fallaron las fuentes de alimentación de los conmutadores de almacenamiento	Crítico, Advertencia, Información	EMS	Falta una fuente de alimentación en el conmutador del clúster. La redundancia se reduce.
La detención de la máquina virtual de almacenamiento se realizó correctamente	Crítico, Advertencia, Información	EMS	La máquina virtual de almacenamiento se detuvo correctamente.
Licencia de replicación de la configuración de SVM no válida	Advertencia	EMS	Falta la licencia de replicación de la configuración de SVM-DR, ha caducado o no se ha aplicado
El sistema no puede funcionar debido a un fallo en el ventilador de la unidad principal	Crítico, Advertencia, Información	EMS	Uno o varios ventiladores de la unidad principal han dejado de funcionar, lo que ha interrumpido el funcionamiento del sistema. Esto podría provocar una posible pérdida de datos.
Demasiada autenticación CIFS	Crítico, Advertencia, Información	EMS	Se han producido muchas negociaciones de autenticación simultáneamente. Hay 256 solicitudes de nuevas sesiones incompletas de este cliente.
Discos sin asignar	Crítico, Advertencia, Información	EMS	El sistema tiene discos sin asignar: se está desperdiciando capacidad.
Estado del volumen sin conexión	Informativo	Métrica	El volumen se ha puesto fuera de línea.
Volumen restringido	Crítico, Advertencia, Información	EMS	Este evento indica que un volumen flexible ha pasado a ser restringido.
Se ha detectado un virus	Crítico, Advertencia, Información	EMS	Un servidor de Vscan informó que un archivo podría estar infectado con un virus.

Alertas de capacidad

Estas alertas indican el consumo de almacenamiento o presión de capacidad.

Nombre de la alerta	Gravedad	Tipo	Descripción
FabricPool la resincronización de la replicación en espejo se completó	Crítico, Advertencia, Información	EMS	El proceso de resincronización del espejo de FabricPool se completó correctamente desde el almacén de objetos principal al almacén de objetos espejo.
FabricPool el límite de uso de espacio está casi alcanzado	Crítico, Advertencia, Información	EMS	El uso total de espacio de FabricPool en todo el clúster de los almacenes de objetos de proveedores con licencia por capacidad ha alcanzado casi el límite de la licencia.
FabricPool se alcanzó el límite de uso de espacio	Crítico, Advertencia, Información	EMS	El uso total de espacio FabricPool en todo el clúster de los almacenes de objetos de proveedores con licencia por capacidad ha alcanzado el límite de la licencia.
Espacio libre en el volumen raíz del nodo insuficiente	Crítico, Advertencia, Información	EMS	El sistema ha detectado que el volumen raíz tiene muy poco espacio disponible.
La memoria del monitor de QoS ha alcanzado su límite máximo	Crítico, Advertencia, Información	EMS	La memoria dinámica de un subsistema de QoS ha alcanzado su límite en el hardware actual de la plataforma.
El cambio automático de tamaño del volumen se realizó correctamente	Crítico, Advertencia, Información	EMS	El volumen se redimensionó automáticamente porque el crecimiento automático del volumen está habilitado.
Volumen completo	Crítico	Métrica	El volumen está lleno en más del 90 %. Libera espacio o añade capacidad para evitar errores de escritura.

Alertas de configuración

Estas alertas indican cambios en la configuración o actualizaciones del inventario.

Nombre de la alerta	Gravedad	Tipo	Descripción
Fuente de alimentación de la estantería de discos detectada	Crítico, Advertencia, Información	EMS	Se ha añadido una fuente de alimentación a la bandeja de discos.
Volumen creado	Información	Métrica	Se ha creado un volumen.
Volumen eliminado	Advertencia	Métrica	Se eliminó un volumen.
Volumen modificado	Información	Métrica	Se ha modificado un volumen.

Nombre de la alerta	Gravedad	Tipo	Descripción
Comprobación de coherencia de WAFL pendiente	Advertencia	EMS	Las comprobaciones de coherencia de WAFL en este agregado superaron el límite horario.

Alertas de rendimiento

Estas alertas indican problemas de latencia o de rendimiento de los nodos.

Nombre de la alerta	Gravedad	Tipo	Descripción
La latencia de NFS en el nodo es elevada	Crítico	Métrica	Las operaciones NFS en este nodo están experimentando una latencia alta (>5000 us).
Pánico en el nodo	Crítico, Advertencia, Información	EMS	El nodo entró en pánico y se reinició.

Alertas de protección

Estas alertas afectan la replicación, la conmutación por error o la recuperación.

Nombre de la alerta	Gravedad	Tipo	Descripción
Se eliminó la snapshot común de la relación Fanout SnapMirror	Crítico, Advertencia, Información	EMS	Se elimina una copia de Snapshot más antigua como parte de una operación de resincronización o actualización de SnapMirror Synchronous.
ONTAP Mediator añadido	Crítico, Advertencia, Información	EMS	El mediador ONTAP se añadió correctamente a este clúster.
El certificado CA de ONTAP Mediator ha caducado	Crítico, Advertencia, Información	EMS	El certificado de la autoridad de certificación (CA) de ONTAP Mediator ha caducado.
El certificado CA de ONTAP Mediator está por caducar	Crítico, Advertencia, Información	EMS	El certificado de la autoridad de certificación (CA) de ONTAP Mediator caducará en los próximos 30 días.
El certificado de cliente de ONTAP Mediator ha caducado	Crítico, Advertencia, Información	EMS	El certificado de cliente de ONTAP Mediator ha caducado.
Caducidad del certificado de cliente de ONTAP Mediator	Crítico, Advertencia, Información	EMS	El certificado de cliente de ONTAP Mediator caducará en los próximos 30 días.

Nombre de la alerta	Gravedad	Tipo	Descripción
No se puede acceder a ONTAP Mediator	Crítico, Advertencia, Información	EMS	No se puede acceder al ONTAP Mediator, ya sea porque se le ha dado un nuevo uso o porque el paquete de Mediator ya no está instalado.
ONTAP Mediator eliminado	Crítico, Advertencia, Información	EMS	El mediador ONTAP se eliminó correctamente de este clúster.
ONTAP Mediator inaccesible	Crítico, Advertencia, Información	EMS	El mediador de ONTAP no es accesible, lo que significa que la conmutación por error de SnapMirror no es posible hasta que se restablezca la conectividad.
El certificado del servidor ONTAP Mediator ha caducado	Crítico, Advertencia, Información	EMS	El certificado del servidor ONTAP Mediator ha caducado.
El certificado del servidor ONTAP Mediator está a punto de caducar	Crítico, Advertencia, Información	EMS	El certificado del servidor ONTAP Mediator caducará en los próximos 30 días.
SnapMirror relación de active sync fuera de sincronización	Crítico, Advertencia, Información	EMS	La relación sincrónica SnapMirror pasó de estar sincronizada a no estarlo. La protección de datos se ve afectada.
SnapMirror la conmutación por error automática no planificada de active sync se completó	Crítico, Advertencia, Información	EMS	La operación de conmutación automática no planificada de la Continuidad de Negocio de SnapMirror (SMBC) se completó.
SnapMirror active sync conmutación por error automática no planificada fallida	Crítico, Advertencia, Información	EMS	La operación de conmutación automática ante fallos no planificados de SnapMirror Business Continuity (SMBC) falló.
SnapMirror la conmutación por error planificada de active sync se completó	Crítico, Advertencia, Información	EMS	La operación de conmutación por error planificada de SnapMirror Business Continuity (SMBC) se completó.
SnapMirror error en la conmutación por error planificada de active sync	Crítico, Advertencia, Información	EMS	La operación de conmutación por error planificada de SnapMirror Business Continuity (SMBC) falló.
Error en la instantánea común de la relación SnapMirror	Crítico, Advertencia, Información	EMS	Se ha producido un error al crear una copia Snapshot común.

Nombre de la alerta	Gravedad	Tipo	Descripción
Error al inicializar la relación de SnapMirror	Crítico, Advertencia, Información	EMS	El comando de inicialización de SnapMirror falla y no se intentarán más reintentos.
SnapMirror relación fuera de sincronización	Crítico, Advertencia, Información	EMS	La relación sincrónica SnapMirror pasó de estar sincronizada a no estarlo. La protección de datos se ve afectada.
Ha fallado el intento de resincronización de la relación SnapMirror	Crítico, Advertencia, Información	EMS	Un intento de sincronización de SnapMirror entre los volúmenes de origen y destino falló.
La instantánea de la relación SnapMirror no se replica	Crítico, Advertencia, Información	EMS	La copia Snapshot para la relación SnapMirror Synchronous no se replicó correctamente.

Alertas de seguridad

Estas alertas indican amenazas o accesos no autorizados.

Nombre de la alerta	Gravedad	Tipo	Descripción
Actividad de ransomware detectada	Crítico, Advertencia, Información	EMS	Para proteger los datos frente al ransomware detectado, se ha creado una copia Snapshot que puede utilizarse para restaurar los datos originales.
Supervisión antiransomware de las máquinas virtuales de almacenamiento	Crítico, Advertencia, Información	EMS	Ha cambiado el estado de protección contra ransomware de la Storage VM.
Acceso no autorizado de un usuario a la carpeta compartida de administración	Crítico, Advertencia, Información	EMS	Un cliente intentó conectarse al recurso compartido con privilegios ONTAP_ADMIN$, pero el usuario que ha iniciado sesión no forma parte de ningún pool de escáneres activo de Vscan en este SVM.
Supervisión anti-ransomware de volúmenes	Crítico, Advertencia, Información	EMS	El estado anti-ransomware de un volumen ha cambiado.

Categorías de cumplimiento de seguridad de clúster en la implementación local de NetApp Console

Utiliza esta referencia para revisar las categorías de cumplimiento de seguridad de los clústeres que se muestran en la implementación local de NetApp Console, incluyendo el valor recomendado y si cada categoría afecta al estado general de cumplimiento.

Estas categorías se basan en las comprobaciones de la postura de seguridad de ONTAP.

Categoría	Qué comprueba la categoría	Valor recomendado	Afecta al cumplimiento normativo en general
FIPS global	Si está activado el modo FIPS 140-2. Cuando está activado, se desactivan TLSv1 y SSLv3 y solo se permiten TLSv1.1 y TLSv1.2.	Habilitado	Sí
Telnet	Si el acceso por Telnet está habilitado. SSH es el método de acceso remoto seguro recomendado.	Deshabilitado	Sí
Configuración insegura de SSH	Si SSH está configurado con algoritmos de cifrado no seguros, como los que comienzan con `cbc`.	No	Sí
Banner de inicio de sesión	Si se ha configurado un banner de inicio de sesión para acceder al sistema.	Habilitado	Sí
Emparejamiento de clústeres	Si la comunicación entre los clústeres de iguales está cifrada. El cifrado debe estar activado tanto en el clúster de origen como en el de destino.	Cifrado	Sí
Protocolo de tiempo de red	Si hay uno o más servidores NTP configurados para el clúster. NetApp recomienda al menos tres servidores NTP para resiliencia.	Configurado	Sí
OCSP	Si está habilitada la validación mediante el Protocolo de estado de certificados en línea (OCSP) para la validación de certificados SSL/TLS.	Habilitado	No
Registro de auditoría remota	Si el reenvío de registros (syslog) está cifrado.	Cifrado	Sí
AutoSupport transporte HTTPS	Si se utiliza HTTPS como protocolo de transporte predeterminado para los mensajes de AutoSupport.	Habilitado	Sí
Usuario administrador predeterminado	Si la cuenta de administrador predeterminada integrada está desactivada.	Deshabilitado	Sí
Usuarios de SAML	Si SAML está configurado para el inicio de sesión único y autenticación compatible con MFA.	No	No
Usuarios de Active Directory	Si se ha configurado la autenticación de Active Directory para el acceso al clúster.	No	No
Usuarios LDAP	Si se ha configurado la autenticación LDAP para el acceso al clúster.	No	No
Usuarios de certificados	Si los usuarios basados en certificados están configurados para iniciar sesión en el clúster.	No	No
Usuarios locales	Si los usuarios locales están configurados para iniciar sesión en el clúster.	No	No
Shell remoto	Si RSH está activado. Se prefiere SSH para un acceso remoto seguro.	Deshabilitado	Sí

Categoría	Qué comprueba la categoría	Valor recomendado	Afecta al cumplimiento normativo en general
MD5 en uso	Si las cuentas de usuario de ONTAP siguen utilizando el algoritmo de hash MD5 en lugar de algoritmos más seguros como SHA-512.	No	Sí
Tipo de emisor del certificado	El tipo de emisor de certificados que utiliza el clúster.	Firmado por CA	No

Categorías de cumplimiento de seguridad de Storage VM en el despliegue local de NetApp Console

Utiliza esta referencia para revisar las categorías de cumplimiento de seguridad de la máquina virtual de almacenamiento (SVM) que se muestran en la implementación local de NetApp Console, incluyendo el valor recomendado y si cada categoría afecta el estado general de cumplimiento.

Estas categorías se basan en las comprobaciones de la postura de seguridad de ONTAP.

Categoría	Qué comprueba la categoría	Valor recomendado	Afecta al cumplimiento normativo en general
Registro de auditoría	Si el registro de auditoría de SVM está activado.	Habilitado	Sí
Configuración insegura de SSH	Si SSH está configurado con algoritmos de cifrado no seguros, como los que comienzan con `cbc`.	No	Sí
Banner de inicio de sesión	Si se ha configurado un banner de inicio de sesión para los usuarios que acceden a los SVM.	Habilitado	Sí
Cifrado LDAP	Si el cifrado LDAP está habilitado.	Habilitado	No
Autenticación NTLM	Si la autenticación NTLM está activada.	Habilitado	No
Firma de la carga útil LDAP	Si la firma de la carga útil LDAP está activada.	Habilitado	No
Configuración de CHAP	Si CHAP está activado.	Habilitado	No
Kerberos V5	Si la autenticación Kerberos V5 está habilitada.	Habilitado	No
Autenticación NIS	Si la autenticación NIS está configurada.	Deshabilitado	No
Estado FPolicy activo	Si FPolicy está creada y activa.	Sí	No
Cifrado SMB activado	Si están activadas las funciones de firma y sellado SMB.	Sí	No
Firma SMB activada	Si la firma SMB está activada.	Sí	No

Conocimiento y soporte

Regístrate para soporte en la implementación local de NetApp Console

Información sobre la implementación local de NetApp Console para esta tarea. Es necesario registrarse en el soporte técnico para recibir soporte técnico específico de NetApp Console y sus soluciones de almacenamiento y servicios de datos. También es necesario registrarse en el soporte técnico para habilitar flujos de trabajo clave para los sistemas Cloud Volumes ONTAP.

El registro para recibir soporte no habilita el soporte de NetApp para el servicio de archivos de un proveedor de nube. Para soporte técnico relacionado con el servicio de archivos de un proveedor de nube, su infraestructura o cualquier solución que use el servicio, consulta la sección "Obtener ayuda" en la documentación de ese producto.

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

Resumen del registro de soporte

Existen dos formas de registro para activar el derecho a la asistencia:

- Registrar el número de serie de tu cuenta de NetApp Console (tu número de serie de 20 dígitos 960xxxxxxxxx que se encuentra en la página de recursos de soporte de la consola).

  Este es tu identificador único de suscripción de soporte para cualquier servicio dentro de la Consola. Cada cuenta de la Consola debe estar registrada.

- Registrar los números de serie de Cloud Volumes ONTAP asociados a una suscripción en el marketplace de tu proveedor de nube (estos son números de serie de 20 dígitos 909201xxxxxxxx).

  Estos números de serie se conocen comúnmente como *números de serie PAYGO* y los genera la NetApp Console en el momento de la implementación de Cloud Volumes ONTAP.

Registrar ambos tipos de números de serie te permite acceder a funciones como abrir tickets de soporte y generar casos de forma automática. El registro se completa añadiendo cuentas del NetApp Support Site (NSS) a la Consola, tal como se describe a continuación.

Registra la consola NetApp para soporte de NetApp

Para registrarte en el soporte y activar el derecho a soporte, un usuario de tu cuenta de NetApp Console debe asociar una cuenta de NetApp Support Site con su inicio de sesión en la Console. Cómo te registras para el soporte de NetApp depende de si ya tienes una cuenta de NetApp Support Site (NSS).

Cliente actual con una cuenta NSS

Si eres cliente de NetApp y tienes una cuenta NSS, solo tienes que registrarte para soporte a través de la Consola.

Pasos

1. Selecciona **Administración** > **Credenciales**.
2. Selecciona **Credenciales de usuario**.
3. Selecciona **Add NSS credentials** y sigue el aviso de autenticación del sitio de soporte de NetApp (NSS).
4. Para comprobar que el proceso de registro se ha realizado correctamente, selecciona el icono de Ayuda y selecciona **Asistencia técnica**.

   La página **Recursos** debería mostrar que tu cuenta de Console está registrada para soporte.

   Ten en cuenta que los demás usuarios de la Consola no verán este mismo estado de registro de soporte si no han asociado una cuenta de NetApp Support Site con su inicio de sesión. Sin embargo, eso no significa que tu cuenta no esté registrada para soporte. Mientras un usuario de la organización haya seguido estos pasos, tu cuenta ya está registrada.

Cliente actual pero sin cuenta NSS

Si ya eres cliente de NetApp y dispones de licencias y números de serie, pero *no* tienes una cuenta NSS, debes crear una cuenta NSS y asociarla a tu inicio de sesión de la Console.

Pasos

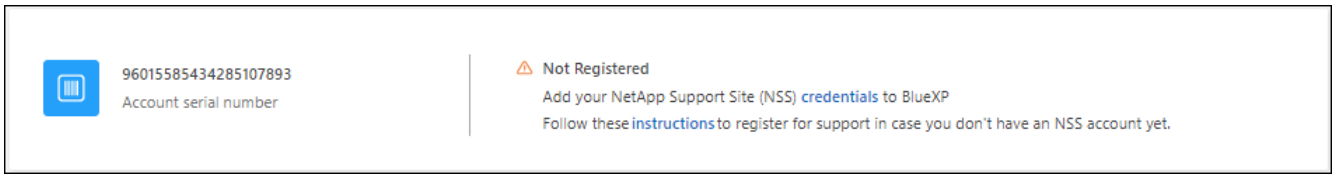
1. Crea una cuenta del sitio de soporte de NetApp completando el "NetApp Formulario de registro de usuario del sitio de soporte"
   a. Asegúrate de seleccionar el nivel de usuario adecuado, que normalmente es **NetApp Customer/End User**.
   b. Asegúrate de copiar el número de serie de la cuenta de Console (960xxxx) utilizado anteriormente en el campo del número de serie. Esto agilizará la tramitación de la cuenta.
2. Vincula tu nueva cuenta de NSS a tus datos de acceso a la Consola siguiendo los pasos que se indican en Cliente actual con una cuenta NSS.

Totalmente nuevo en NetApp

Si acabas de llegar a NetApp y no tienes una cuenta de NSS, sigue cada paso a continuación.

Pasos

1. En la esquina superior derecha de la consola, selecciona el icono de Ayuda y selecciona **Soporte**.
2. Busca el número de serie de tu ID de cuenta en la página de registro de soporte.



3. Accede a "NetApp sitio de registro de soporte" y selecciona **I am not a registered NetApp Customer**.
4. Rellena los campos obligatorios (los que tienen un asterisco rojo).
5. En el campo **Línea de productos**, selecciona **Cloud Manager** y luego selecciona tu proveedor de facturación correspondiente.
6. Copia el número de serie de tu cuenta del paso 2 anterior, completa la verificación de seguridad y luego confirma que leíste la política de privacidad global de NetApp.

Se envía inmediatamente un correo electrónico al buzón proporcionado para finalizar esta transacción segura. Asegúrate de revisar tus carpetas de correo no deseado si el correo electrónico de validación no llega en unos minutos.

7. Confirma la acción desde el propio correo electrónico.

   Al confirmar, envías tu solicitud a NetApp y se te recomienda que crees una cuenta de NetApp Support Site.

8. Crea una cuenta del sitio de soporte de NetApp completando el "NetApp Formulario de registro de usuario del sitio de soporte"
   a. Asegúrate de seleccionar el nivel de usuario adecuado, que normalmente es **NetApp Customer/End User**.
   b. Asegúrate de copiar el número de serie de la cuenta (960xxxx) utilizado anteriormente en el campo del número de serie. Esto agilizará la tramitación.

Después de que termines

NetApp debería ponerse en contacto contigo durante este proceso. Este es un ejercicio de incorporación único para nuevos usuarios.

Una vez que tengas tu cuenta del sitio de soporte de NetApp, vincula dicha cuenta a tu nombre de usuario de la consola siguiendo los pasos que se indican en Cliente actual con una cuenta NSS.

Asociar credenciales de NSS para el soporte técnico de Cloud Volumes ONTAP

Es necesario vincular las credenciales del sitio de soporte de NetApp a tu cuenta de la Console para habilitar los siguientes flujos de trabajo clave de Cloud Volumes ONTAP:

- Registrar sistemas Cloud Volumes ONTAP de pago por uso para soporte

  Es necesario facilitar tu cuenta de NSS para activar el soporte técnico de tu sistema y poder acceder a los recursos de soporte técnico de NetApp.

- Implementación de Cloud Volumes ONTAP cuando traes tu propia licencia (BYOL)

  Es necesario que facilites tu cuenta de NSS para que la Console pueda cargar tu clave de licencia y activar la suscripción durante el periodo que hayas adquirido. Esto incluye actualizaciones automáticas para las renovaciones del periodo.

- Actualizar el software Cloud Volumes ONTAP a la última versión

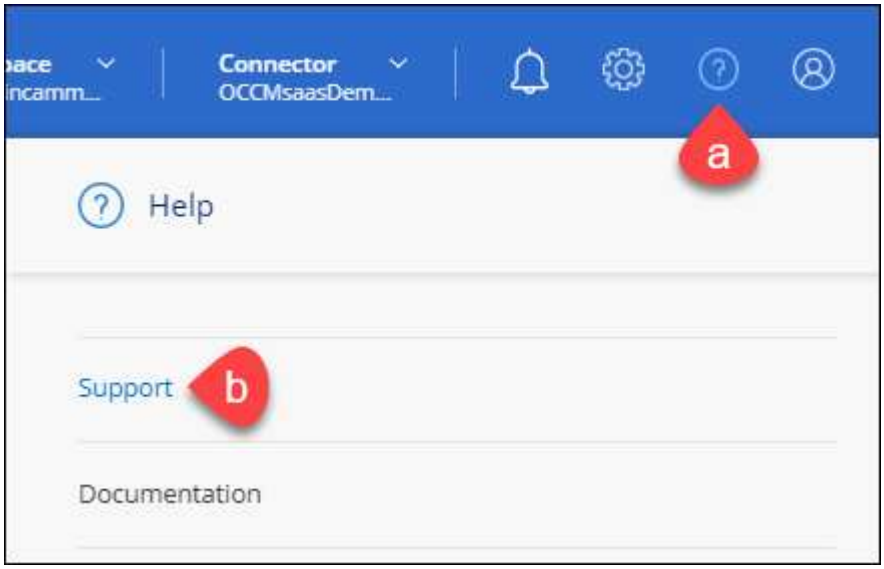
La vinculación de las credenciales de NSS con tu cuenta de NetApp Console es diferente de la cuenta de NSS que está asociada con el inicio de sesión de un usuario de Console.

Estas credenciales de NSS están asociadas a tu ID de cuenta específico de la Console. Los usuarios que pertenezcan a la organización de la Console pueden acceder a estas credenciales desde **Support > NSS Management**.

- Si tienes una cuenta de nivel de cliente, puedes añadir una o varias cuentas NSS.
- Si tienes una cuenta de socio o de distribuidor, puedes añadir una o varias cuentas NSS, pero no se pueden añadir junto con cuentas de cliente.

Pasos

1. En la esquina superior derecha de la consola, selecciona el icono de Ayuda y selecciona **Soporte**.



2. Selecciona **NSS Management > Add NSS Account**.
3. Cuando se te solicite, selecciona **Continuar** para que se te redirija a una página de inicio de sesión de Microsoft.

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

4. En la página de inicio de sesión, introduce tu dirección de correo electrónico registrada en el sitio de soporte de NetApp y tu contraseña para realizar el proceso de autenticación.

   Estas acciones permiten que la consola utilice tu cuenta NSS para cosas como la descarga de licencias, la verificación de actualizaciones de software y futuros registros de soporte.

   Ten en cuenta lo siguiente:

   - La cuenta NSS debe ser una cuenta de cliente (no una cuenta de invitado ni una cuenta temporal). Puedes tener varias cuentas NSS de cliente.
   - Solo puede haber una cuenta NSS si se trata de una cuenta de nivel de partner. Si intentas añadir cuentas NSS de nivel de cliente y ya existe una cuenta de nivel de partner, aparecerá el siguiente mensaje de error:

     «El tipo de cliente NSS no está permitido para esta cuenta, ya que ya hay usuarios NSS de otro tipo»

   Lo mismo ocurre si ya tienes cuentas NSS a nivel de cliente y intentas añadir una cuenta a nivel de partner.

   - Una vez que hayas iniciado sesión correctamente, NetApp almacenará el nombre de usuario de NSS.

     Este es un ID generado por el sistema que se asocia a tu correo electrónico. En la página **NSS Management**, puedes mostrar tu correo electrónico desde el menú ••• .

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

     Al utilizar esta opción, se te pedirá que vuelvas a iniciar sesión. Ten en cuenta que el token de estas

cuentas caduca a los 90 días. Se publicará una notificación para avisarte de esto.

Obtén ayuda con la implementación local de NetApp Console

NetApp Console información sobre la implementación local para esta tarea. NetApp ofrece soporte para NetApp Console y sus servicios en la nube de diversas formas. Hay disponibles amplias opciones gratuitas de autoayuda las 24/7, como artículos de la base de conocimientos (KB) y un foro de la comunidad. Tu registro de soporte incluye soporte técnico remoto a través de tickets web.

Obtén soporte para el 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, consulta la documentación de ese producto.

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

Para recibir soporte técnico específico para NetApp y sus soluciones de almacenamiento y servicios de datos, utiliza las opciones de soporte descritas a continuación.

Utiliza las opciones de autoservicio

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 ahora.

- "Base de conocimientos"

  Busca en la base de conocimientos de NetApp para encontrar artículos útiles y solucionar problemas.

- "Comunidades"

  Únete a la comunidad de NetApp Console para seguir las discusiones en curso o crear nuevas.

Crea un caso con el soporte de NetApp

Además de las opciones de autoayuda mencionadas anteriormente, puedes trabajar con un especialista de soporte de NetApp para resolver cualquier problema después de que actives el soporte.

Antes de empezar

- Para usar la función **Crear un caso**, primero debes asociar tus credenciales del sitio de soporte de NetApp con tu inicio de sesión en la consola. "Aprende a gestionar las credenciales asociadas a tu inicio de sesión en la consola".
- Si vas a abrir un caso para un sistema ONTAP que tiene un número de serie, entonces tu cuenta NSS debe estar asociada a ese número de serie.

Pasos

1. En la consola NetApp, selecciona **Ayuda > Soporte**.
2. En la página **Recursos**, elige una de las opciones disponibles en Soporte técnico:

   a. Selecciona «Llámanos» si deseas hablar con alguien por teléfono. Se te redirigirá a una página en netapp.com en la que figuran los números de teléfono a los que puedes llamar.

   b. Selecciona **Crear un caso** para abrir un ticket con un especialista de soporte técnico de NetApp:

      - **Servicio**: Selecciona el servicio con el que está asociado el problema. Por ejemplo, **NetApp Console** cuando se trate de un problema de soporte técnico con flujos de trabajo o funcionalidad dentro de la Console.
      - **Sistema**: Si es aplicable al almacenamiento, selecciona **Cloud Volumes ONTAP** o **On-Prem** y luego el entorno de trabajo asociado.

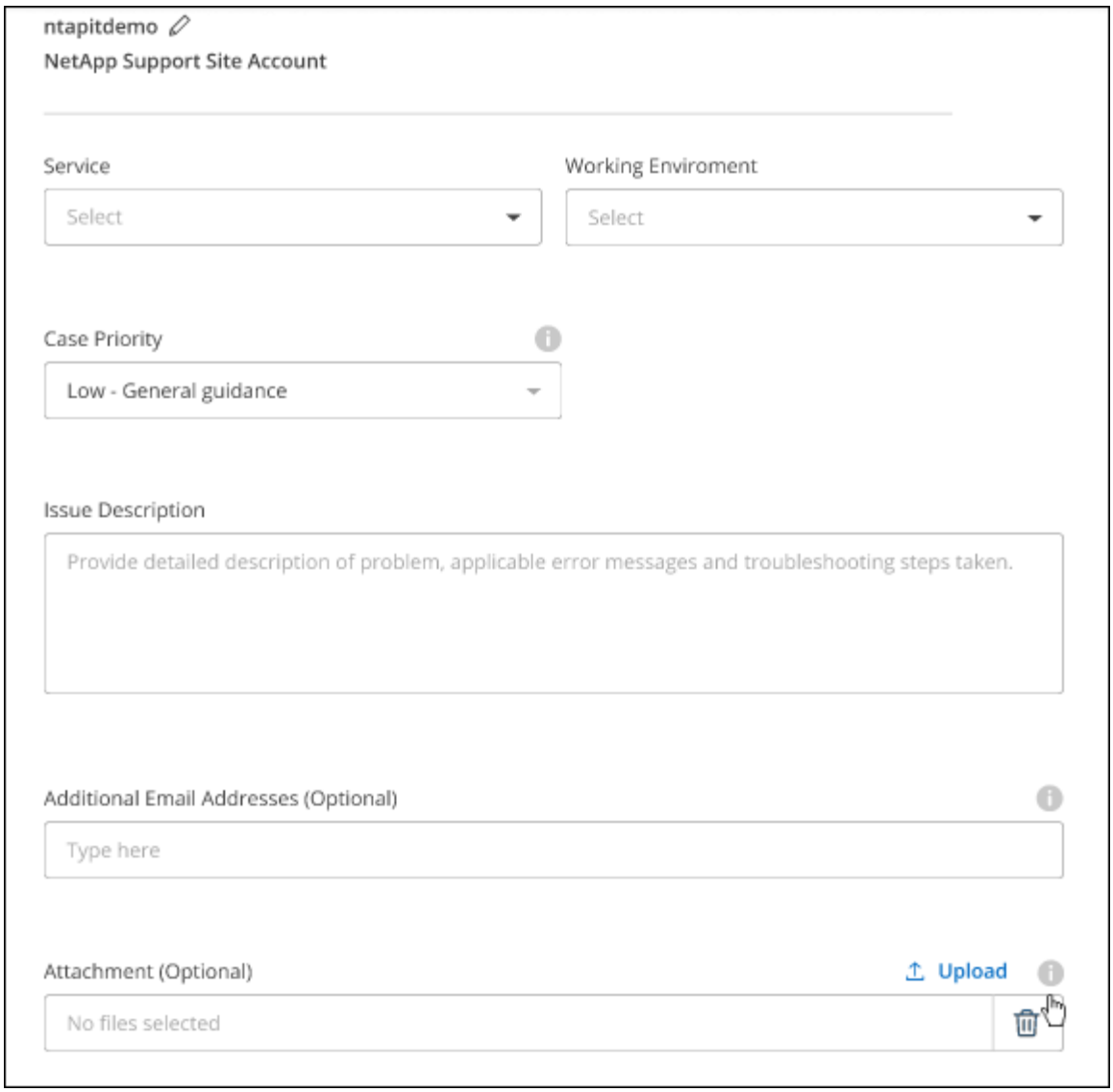
        La lista de sistemas está dentro del ámbito de la organización de la Console y del agente de la Console que tú has seleccionado en el banner superior.

      - **Prioridad del caso**: Elige la prioridad del caso, que puede ser baja, media, alta o crítica.

        Para obtener más detalles sobre estas prioridades, pasa el mouse por encima del icono de información junto al nombre del campo.

      - **Descripción del problema**: Proporciona una descripción detallada de tu problema, incluyendo cualquier mensaje de error aplicable o los pasos de resolución de problemas que realizaste.
      - **Direcciones de correo electrónico adicionales**: Introduce direcciones de correo electrónico adicionales si deseas informar a otra persona sobre este asunto.
      - **Archivo adjunto (opcional)**: Sube hasta cinco archivos adjuntos, uno a la vez.

        Los archivos adjuntos tienen un límite de 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 que termines

Aparecerá una ventana emergente con el número de tu caso de soporte. Un especialista de soporte de NetApp revisará tu caso y se pondrá en contacto contigo pronto.

Para consultar el historial de tus casos de soporte, puedes seleccionar **Configuración > Cronología** y buscar las acciones denominadas "crear caso de soporte". Un botón situado en el extremo derecho te permite expandir la acción para ver los detalles.

Es posible que te aparezca el siguiente mensaje de error al intentar crear un caso:

«No estás autorizado a crear un caso contra el servicio seleccionado»

Este error podría significar que la cuenta NSS y la empresa de registro a la que está asociada no es la misma empresa de registro para el número de serie de la cuenta de NetApp Console (es decir, 960xxxx) o el número de serie del entorno de trabajo. Puedes solicitar asistencia usando una de las siguientes opciones:

- Envía un caso no técnico a https://mysupport.netapp.com/site/help

Administra tus casos de soporte técnico

Puedes ver y gestionar los casos de soporte activos y resueltos directamente desde la NetApp Console. Puedes gestionar los casos asociados a tu cuenta NSS y a tu empresa.

Ten 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 has facilitado.
  - La vista de la derecha muestra el total de casos abiertos en los últimos 3 meses a nivel de tu empresa según tu cuenta de usuario NSS.

  Los resultados en la tabla reflejan los casos relacionados con la vista que seleccionaste.
- Puedes añadir o eliminar las columnas que te interesen y puedes filtrar el contenido de columnas como Prioridad y Estado. Otras columnas solo permiten ordenar.

  Consulta los pasos que se indican a continuación para obtener más detalles.
- A nivel de cada caso, ofrecemos la posibilidad de actualizar las notas del caso o cerrar un caso que aún no esté en estado Closed o Pending Closed.

Pasos

1. En la consola NetApp, selecciona **Ayuda > Soporte**.
2. Selecciona **Case Management** y si te lo piden, añade tu cuenta NSS a la NetApp Console.

   La página **Gestión de casos** muestra los casos abiertos relacionados con la cuenta NSS asociada a tu cuenta de usuario de la Console. Esta es la misma cuenta NSS que aparece en la parte superior de la página **Gestión NSS**.
3. Si lo deseas, puedes modificar la información que se muestra en la tabla:
   - En **Casos de la organización**, selecciona **Ver** para ver todos los casos asociados con tu empresa.
   - Modifica el intervalo de fechas eligiendo un intervalo exacto o seleccionando otro periodo de tiempo.
   - Filtra el contenido de las columnas.
   - Cambia las columnas que aparecen en la tabla seleccionando y luego elige las columnas que te gustaría mostrar.
4. Gestiona un caso existente seleccionando y eligiendo una de las opciones disponibles:
   - **Ver caso**: Ver todos los detalles sobre un caso específico.
   - **Actualizar notas del caso**: Facilita más detalles sobre tu problema o selecciona **Subir archivos** para adjuntar hasta un máximo de cinco archivos.

     Los archivos adjuntos tienen un límite de 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**: Indica los motivos por los que vas a cerrar el caso y selecciona **Cerrar caso**.